Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray Into Facial Recognition Technology From Haunting Consumer Privacy Rights Forever

Rosie Brinckerhoff *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. Executive Editor & Notes Editor, *Federal Communications Law Journal*, 2017–2018. B.A., Political Science, Minor in Journalism, University of Delaware, 2014. This Note is dedicated to my father, Clarke W. Brinckerhoff, the most brilliant and humble man I know. His love for the law and penchant for fairness are what inspired me to pursue a legal career. It is only because he thought I could succeed in this field that I even dared to try. I would like to extend a special thank you to everyone who feigned interest in hearing me ramble about Facebook over the past year and a half, but especially to my patient and loving mother, Judy Brinckerhoff. Many thanks to the staff of the *Federal Communications Law Journal* for their patient and meticulous editing. I would also like to thank Kara Romagnino for asking me the tough questions throughout my writing process and for providing extensive feedback on my many drafts. Any unprincipled deviations in this Note are my own.

I. INTRODUCTION

The rapid explosion in the number of social media companies utilizing and implementing facial recognition technology has introduced many privacy risks associated with collecting and storing consumer biometric[1] data for commercial use.[2] The fundamental issue stems from the fact that "[i]n the U[.]S[.], there is no single, comprehensive federal law regulating privacy and the collection, use, . . . and security of personal information."[3] Rather, the United States has a piecemeal system with respect to consumer data privacy, consisting of industry-specific federal privacy laws,[4] state privacy laws,[5] and

1. *See* Information Security Law § 1.01(6)(d) (LEXIS 2016) ("Translated literally, 'biometrics' means 'life measurement' - *bios* is Greek for 'life'; *metricus* is Latin for 'relating to measurement.' Biometrics can relate to a variety of means for establishing an individual's identity. Popular biometric methods of authentication include fingerprints, voice prints, iris scanning, and facial recognition.").

2. For a general discussion of privacy concerns manifesting from Facebook's use of facial recognition technology, *see generally* ELECTRONIC PRIVACY INFORMATION CENTER, IN THE MATTER OF FACEBOOK, INC. AND THE FACIAL IDENTIFICATION OF USERS, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [https://perma.cc/58TB-RQPB].

3. Ieuan Jolly, *US Privacy and Data Security Law: Overview*, LOEB & LOEB LLP, (July 1, 2016), https://blog.richmond.edu/lawe759/files/2016/08/US-Privacy-and-Data-Security-Law-Overview.pdf [https://perma.cc/9T6T-7M8N].

4. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY REPORT 33 (2015), http://www.gao.gov/assets/680/671764.pdf [https://perma.cc/3LVE-YFLG] ("Certain federal laws do address the collection, use, and sale of personal information by private-sector companies, as discussed earlier. These laws could potentially restrict, in certain circumstances, the collection of facial images, which are used to build a database for use with facial recognition technology. For example, provisions in the Driver's Privacy Protection Act restrict state motor vehicle bureaus from selling drivers' license photographs and associated information to private parties. In addition, the Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act potentially could restrict the ability of banks and health care providers to share data collected with facial recognition technology if those data were to fall within the laws' definitions of protected information. However, the reach of these laws is limited because they generally apply only for specific purposes, in certain situations, to certain sectors, or to certain types of entities.").

5. Illinois leads the way in protecting consumer privacy with respect to biometric identifiers. Before collecting or storing any biometric identifying information, Illinois statutorily requires that a company: "(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." *See generally* Illinois' Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b) (2008), http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 [https://perma.cc/NH9E-J5R3]. *See infra* note 40 for more information on other state-specific privacy laws.

best practice guides[6] from various governmental agencies.[7] Fittingly, this fragmented approach to regulating consumer data privacy has best been described as a "patch-work quilt."[8] With a disjointed legislative framework and no broad federal law in place to regulate the collection and distribution of biometric data, consumer privacy is becoming increasingly vulnerable.[9]

As a result, operating with no real legal restraint and only under conditions of self-regulation,[10] social media companies are well-positioned to take advantage of unsuspecting consumers using social networking sites and applications.[11] As one legal scholar succinctly stated "we cannot justify

---

6. In 2012, the FTC released its first and only "Best Practices Guide" for companies utilizing facial recognition technology, offering merely suggestions that companies are essentially free to ignore. *See Federal Trade Commission*, Best Practices for Common Uses of Facial Recognition Technologies (Oct. 12, 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf) [https://perma.cc/KD8G-43TK]; *cf.* Charles E. MacLean, *It Depends: Recasting Internet Clickwrap, Browsewrap, "I Agree," and Click-Through Privacy Clauses as Waivers of Adhesion*, 65 CLEV. ST. L. REV. 43, 52–53 (2016), http://engagedscholarship.csuohio.edu/clevstlrev/vol65/iss1/7 [https://perma.cc/B6CT-BWWS] ("Even the FTC's data privacy enforcement actions have been largely ineffective. When the FTC compelled Google and Facebook to more clearly disclose to consumers the private consumer data they were capturing and selling to others, the result was not more consumer protection, but merely more dense and indecipherable privacy disclosures that most users simply click through without reading— certainly without understanding") (citing Cameron Scott, *Less than Half of Facebook, Google Users Understand Sites' Privacy Policies*, COMPUTERWORLD (May 4, 2012), http://www.computerworld.com/article/2503822/data-privacy/less-than-half-of-facebook-- google-users-understand-sites--privacy-policies.html [https://perma.cc/LGR6-WWJN])).

7. Jolly, *supra* note 3.

8. Rosemary P. Jay, Lisa J. Sotto & Aaron P. Simpson, *Data Protection & Privacy 2015*, HUNTON & WILLIAMS PG. 208 (accessed Apr. 4, 2017), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf [https://perma.cc/93JX-Q9ZE].

9. *See, e.g.*, Chris Tomlinson, *Loss of internet data privacy should concern business, consumers*, HOUSTON CHRONICLE (Apr. 3, 2017), http://www.houstonchronicle.com/business/columnists/tomlinson/article/Business-should-worry-about-lost-data-privacy-11041215.php [https://perma.cc/4QSU-SHX5] ("This isn't just about whether you watch cat videos or visit porn sites. The most frightening part is that the repeal of internet privacy protections is only the beginning of a process that will be more intrusive than any strip search or home invasion . . . In a more connected world, when every electric device is connected to the internet, the effect could be profound and disturbing.").

10. *See, e.g.*, *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 12 (2012) (testimony of Jennifer Lynch of the Electronic Frontier Foundation), https://ssrn.com/abstract=2134497 [https://perma.cc/N7R9-XPCQ], ("[I]ndustry self- regulation and consumer control are not enough to protect against critical privacy and security risks inherent in facial recognition data collection.").

11. *See, e.g.*, Maelle Gavet, *The data says Google and Facebook need regulating*, WIRED (Mar. 5, 2015), http://www.wired.co.uk/article/data-google-facebook [https://perma.cc/WJL6-69TS] ("By assuming companies can be trusted to use our data responsibly, we are complicit in the notion that self-regulation will suffice -- and that we tamper with these innovators, by binding them up in regulation, at our peril. This is dangerous. It simply isn't acceptable for the likes of Google, Facebook, Amazon and others, which amass data by the terabyte, to say,

leaving the protection of consumers in their henhouses to the foxes who are collecting and profiting from the aggregation, sale, and resale of all this formerly private consumer data."[12]

Although the problem is much more pervasive than one company alone, this note is limited to Facebook, arguably the goliath of social media due to its 1.86 billion[13] users. By maintaining vastly overreaching user agreements and privacy policies, to which consumers are required to assent on a take it or leave it basis, Facebook is essentially demanding that consumers choose between signing away any last semblance of their privacy or being ostracized from a growing community of billions of social media users worldwide.[14]

Because technological innovation and Internet reliance are unlikely to come to a halt, prospective action needs to be taken to protect consumer privacy before it is too late.[15] As Facebook continues its quest into storing, selling, and sharing arguably anything and everything it can about its users in order to turn a profit, more stringent laws and regulations governing what companies are permitted to collect, store, and use are more necessary now than ever.[16] However, because comprehensive federal consumer privacy legislation is unlikely to be enacted anytime soon,[17] this note serves to argue

---

"Don't worry, your information's safe with us as all sorts of rules protect you" -- when all evidence suggests otherwise.").

12. Charles E. MacLean, *It Depends: Recasting Internet Clickwrap, Browsewrap, "I Agree," and Click-Through Privacy Clauses as Waivers of Adhesion*, 65 CLEV. ST. L. REV. 43, 49 (2016), http://engagedscholarship.csuohio.edu/clevstlrev/vol65/iss1/7 [https://perma.cc/B6CT-BWWS].

13. *Company Info*, FACEBOOK, (last revised Dec. 2016), http://newsroom.fb.com/company-info [https://perma.cc/E3GK-YUTB]/ (accessed Apr. 1, 2017).

14. *See, e.g.*, Stacey Higginbotham, *Companies need to share how they use our data. Here are some ideas*, FORTUNE MAGAZINE (July 6, 2015), http://fortune.com/2015/07/06/consumer-data-privacy/ [https://perma.cc/6YDH-Y69Y] ("Currently, the choice is often pretty black and white. You accept the onerous terms of service (which are often presented in convoluted user agreements someone clicks through on their way to download the app after purchasing a new device) or you don't get to use the service.").

15. *See, e.g.*, Mark Weinstein, *Terms and Conditions May Apply Documentary: A Must See Horror Film*, THE HUFFINGTON POST (Aug. 2, 2013), http://www.huffingtonpost.com/mark-weinstein/terms-and-conditions-may-_b_3692883.html [https://perma.cc/N86Y-ZUMN] (acknowledging that "anonymity isn't profitable . . . [which] has driven Internet monoliths such as Google and Facebook to turn the Internet into a cog that turns us into a real-time surveillance state and George Orwell into a[] historian and prognosticator instead of an acclaimed fiction writer").

16. *See, e.g.*, Gavet, *supra* note 11 ("The history of business has shown that companies usually only regulate themselves if they're forced to by legislation, or out of self-interest -- often in the shape of a marketable message that will help sell more products. Not only is self-regulation largely a fantasy, but repeated scandals across multiple industries have proved that companies are fundamentally incapable of self-regulating for the greater good.").

17. *See Federal Trade Commission*, Privacy & Security in a Connected World, Staff Report (Jan. 2015) pg. vii , https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/TX3V-EFXY] (although the FTC recommended in 2015 "for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers

that intervention by the California judiciary is the best alternative in protecting consumer privacy from Facebook's overbearing Terms of Service and Data Policy. In addition to Facebook's forum selection clause mandating that any claims be resolved under California law "in the U.S. District Court for the Northern District of California or a state court located in San Mateo County,"[18] California provides a uniquely situated forum for judicial resolution due to its proximity and history with technology litigation.[19]

Although "[t]he California legislature has introduced several bills that would directly regulate biometrics collection . . . due in part to industry pushback, none of these laws has moved out of the legislature."[20] For example, legislation proposed in 2011 in the California Senate "which would [have] require[d] a company that collects or uses 'sensitive information,' including biometric data, to allow users to opt-out of its collection, use, and storage [] faced stiff opposition from technology companies and their trade organizations."[21] In an opposition letter written in response to the proposed state legislation, the signing companies argued that "[p]rohibiting the collection and use of this data would severely harm future innovation in the state and harm consumers."[22]

Despite the fact that the industry desires to proceed unregulated in this modern-day race for data aggregation, the argument that consumer privacy comes at the expense of innovation is necessarily skewed. It is entirely possible to protect consumer privacy without stifling and impeding technological innovation; accurately stated by Federal Communications Commission (FCC) Enforcement Bureau Chief Travis LeBlanc, "[p]rivacy and innovation are not incompatible."[23] Because "[i]t is no longer enough to justify privacy invasions as technologically inevitable or as essential to the American economy,"[24] California courts have a critical opportunity to

---

when there is a security breach," Congress has not acted towards implementing broad consumer data privacy legislation).

18. FACEBOOK, *Terms of Service, Section 15*, https://www.facebook.com/terms.php (accessed Apr. 10, 2017).

19. *See, e.g.*, Campbell et al v. Facebook Inc., Case No.: 4:13-cv-5996 (N.D. Cal. 2013) (regarding Facebook's alleged interception of private user messages for purposes of data mining and sharing with third parties); Singh v. Google, No. 16-cv-03734-BLF * 2 (N.D. Cal. 2016) (regarding Google's alleged failure "to prevent invalid clicks on unspecified AdWords advertisements"). Additionally, a number of technology giants, such as Google and Apple, have forum selection clauses specifying that claims are to be litigated exclusively in California. (*See* Google, Terms of Service, https://www.google.com/policies/terms/ (accessed Feb. 15, 2018); Apple, Media Services Terms and Conditions, https://www.apple.com/legal/internet-services/itunes/us/terms.html (accessed Feb. 15, 2018).

20. Lynch, *supra* note 10, at 21.

21. *Id*.

22. Opposition Letter to Sen. Alan Lowenthal (Apr. 27, 2011), http://static.arstechnica.com/oppositionletter.pdf.

23. *See* Press Release, Federal Communications Commission, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf (LeBlanc further noted that "[c]onsumers care about privacy and should have a say in how their personal information is used, especially when it comes to who knows what they're doing online").

24. MacLean, *supra* note 12, at 45.

proactively remedy the growing divide between reasonably sound consumer privacy policy and rapidly emerging technology endeavors.[25] Industry pushback and failure of the California legislature to pass a proper consumer privacy bill should not bring consumer privacy efforts to a grinding halt, especially when the state constitution has sufficiently teed up California courts to address the issue.

As such, this note will demonstrate why California courts are perfectly positioned to set the standard for pro-consumer, pro-privacy user agreements by holding Facebook's Terms of Service and Data Policy unconscionable due to the company's non-consensual deployment of facial recognition technology to collect its users' biometric data. [26]

Section II of this note will provide a brief technical overview of facial recognition technology and its associated privacy implications, as well as a background discussion on Facebook's current capabilities with facial recognition technology. Section III of this note will outline the doctrine of unconscionability under California law, examining the requisite elements and interplay between procedural and substantive unconscionability. This section will also include an analysis of how Facebook fails to explicitly mention and explain its biometric data collection practices in its ambiguous and overreaching Terms of Service and Data Policy, arguing that Facebook's non-consensual collection of this sensitive data is unconscionable pursuant to California law. Finally, Section IV of this note will conclude with an explanation of why California courts are in the best position to set a standard for Terms of Service and Data Policy agreements that adequately protect consumer privacy without hindering private-sector technological innovation. Apart from discussing how and why courts should properly reach a finding of unconscionability with respect to Facebook's biometric data collection practices, this section will also propose two additional solutions, one under state constitutional law and one under state tort law, in an effort to demonstrate the many legal tools the California judiciary has at its disposal to safeguard sensitive consumer biometric data.

25. *See generally* MacLean, *supra* note 12.

26. California courts are the only hope for consumers in adequately addressing this issue, as Facebook includes a forum clause in its Terms of Service agreement requiring any and all disputes and litigation to be handled in California. Pursuant to Section 15 of Facebook's Statement of Rights and Responsibilities, "[t]he laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions." *Terms*, FACEBOOK (last revised Jan. 30, 2015), https://www.facebook.com/terms.php [https://perma.cc/U848-M6QV] (accessed Apr. 3, 2017).

II. BACKGROUND: A BRIEF GUIDE TO FACIAL RECOGNITION TECHNOLOGY

A. Facial Recognition Technology – A Brief, Technical Overview

Facial recognition technology is most simply described as a biometric technology resource "which identifies individuals by measuring and analyzing their physiological or behavioral characteristics."[27] Designed to mimic and advance the human ability to recognize and identify faces,[28] computer facial recognition technology systems are capable of holding and analyzing an enormous amount of facial data imaging.[29] To illustrate this concept, while the human brain has a limited ability in the number of faces it can precisely recall,[30] a single server computer can search over 10 million records in less than 10 seconds.[31]

The exact mechanics of a facial recognition technology system are far beyond the scope of this note.[32] However, a brief explanation of the fundamental technology is necessary in order to understand the legal argument asserted herein. Accordingly, "[t]here are generally four basic components to a facial recognition technology system: a camera to capture an image, an algorithm to create a faceprint (sometimes called a facial template), a database of stored images, and an algorithm to compare the captured image to the database of images or a single image in the database."[33]

After uploading a photograph, a machine learning algorithm is trained to recognize any number of "specific points (called landmarks) that exist on every face—the top of the chin, the outside edge of each eye, the inner edge of each eyebrow" and more.[34] This information is used to create a facial template, which "is a reduced set of data that represents the unique features of [a person's] face."[35] The template is then compared against other stored

27. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 2.

28. *See* Danna Voth, *Face recognition technology*, 18 IEEE INTELLIGENT SYSTEMS 3, 4–7 (May-June 2003), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1200719 [https://perma.cc/79MK-RQAZ].

29. WENYI ZHAO & RAMA CHELLAPPA, FACE PROCESSING: ADVANCED MODELING AND METHODS, 8, 9 (Academic Press 2006).

30. *Id*.

31. *See* Michael Petrov, *Law Enforcement Applications of Forensic Face Recognition*, MORPHOTRUST USA, 12 (Sept. 2012), http://www.planetbiometrics.com/creo_files/upload/article-files/whitepaper_facial_recognition_morphotrust.pdf [https://perma.cc/UJ6M-DH4B].

32. For a thorough explanation and inquiry into facial recognition technology, *see generally* STAN Z. LI & ANIL K. JAIN, HANDBOOK OF FACIAL RECOGNITION, (2d ed. Springer 2011).

33. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 3.

34. Adam Geitgey, *Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning*, MEDIUM (July 24, 2016), https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78#.gz60g6v3i [https://perma.cc/U9NQ-4TXM].

35. JOHN D. WOODWARD, JR. ET AL., BIOMETRICS: A LOOK AT FACIAL RECOGNITION, 3–4 RAND (2003).

images in the system database by way of a process that can then be used for either identification or verification purposes.[36]

Although in the past facial recognition technologies have been predominantly used by law enforcement agencies and government entities,[37] "commercial interest and [private] investment in facial recognition technology have grown as the technology has become more accurate and less costly, with new applications being developed for consumers and businesses."[38] With an ever-increasing demand, the facial recognition technology market is predicted to reach $2.67 billion in 2022.[39] However, the emerging interest and rapid growth in companies using facial recognition technology for commercial purposes creates novel consumer privacy implications and concerns that have not been addressed through federal legislation.[40]

B. Privacy Implications of Facial Recognition Technology

The greatest concern in increased use of facial recognition technology is the loss of privacy to consumers.[41] This unease stems from the fact that "if its use becomes widespread, businesses or individuals may be able to identify almost anyone in public without their knowledge or consent."[42] Because facial recognition technology essentially maps and codifies a person's facial

36. *Id*. ("In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database – that of the claimed identity.").

37. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 7 (citing *The Current and Future Applications of Biometric Technologies: Hearing Before the Subcomm. on Research and Tech. of the H. Comm. on Science, Space and Tech.*, 113th Cong. 1 (2013) (statement of John Mears, Board Member, International Biometrics & Identification Association)).

38. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4, at 7, (citing FTC, *supra* note 6.).

39. *See Facial Recognition Market Expected to Reach US$ 2.67 Bn by 2022 Globally*, TRANSPARENCY MARKET RESEARCH, (Jul. 23, 2015), http://www.transparencymarketresearch.com/pressrelease/facial-recognition-market.htm [https://perma.cc/92JU-ECGN].

40. Three states, Illinois, Texas and Washington, have enacted laws regulating the collection, use and retention of consumer biometric data, signaling a shift towards a more state-based regulatory framework. However, this piecemeal state-by-state approach raises a host of other concerns outside the scope of this note. For a discussion of the Illinois, Texas and Washington biometric laws, *see generally* Ted Claypoole &Cameron Stoll, Developing Laws Address Flourishing Commercial Use of Biometric Information, AMERICAN BAR ASSOCIATION (May 2016), https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html [https://perma.cc/C84P-GTGW].

41. *See, e.g.*, NANCY YUE LIU, BIO-PRIVACY; PRIVACY REGULATIONS AND THE CHALLENGE OF BIOMETRICS, 78 (Routledge Taylor & Francis Group 2012) ("It will generally not be a difficult task to link, directly or indirectly, a biometric identifier to other personal data . . . [i]f personal information could be linked and identified using the biometric data, one's ability to remain anonymous would be severely diminished." (citation omitted)).

42. *See* Information Security Law, *supra* note 1.

geometry,[43] "[p]rivacy advocates essentially argue that conversion of facial features to machine-readable data points eliminates one's ability to voluntarily choose to disclose ones identity to the public and such features become a resource that others control."[44]

To illustrate this point, California-based facial recognition technology company FaceFirst allows retailers to upload photographs of their best customers, repeat shoplifters, or other persons of interest into a facial database. When a person in the database enters the store, the system immediately notifies the owner and sends an "alert that includes their picture and all biographical information of the known individual."[45] FaceFirst touts itself as a beneficial service for retailers, casinos, and stadiums alike that can enhance customer service while concurrently cracking down on crime and shoplifting.[46] However, FaceFirst's quest to maximize commercial profits and enhance customer service fails to take into account whether or not a consumer wants to be recognized and identified. With no consumer privacy law in place to govern, retailers are under no legal obligation to disclose its use of the facial recognition technology.

Further, the lengths to which facial recognition technology may be employed are extensive and far-reaching. For example, in Russia, a facial recognition app called FindFace enables consumers to photograph a stranger and discern his or her identity with up to 70% accuracy.[47] This application draws striking similarities to Recognizr, a Swedish mobile application that enables users to point a smartphone camera at another person, after which "[a] cloud server conducts the facial recognition [ ] and sends back the subject's name as well as links to any social networking sites the person has provided access to."[48]

---

43. *See* Woodward, *supra* note 35 ("Because a person's face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (i.e. the subject does not necessarily know he has been observed).").

44. *See* Information Security Law, *supra* note 1.

45. *See* FaceFirst, http://www.facefirst.com/services/retail (accessed Nov. 18, 2016); *accord* Natasha Singer, *When No One Is Just a Face In The Crowd*, N.Y. TIMES (Feb. 1, 2014), https://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html [https://perma.cc/92UQ-HS3F].

46. *See Face Recognition for Retail Stores*, FACEFIRST, https://www.facefirst.com/industry/retail-face-recognition/ [https://perma.cc/WW9M-EJZY] (accessed Apr. 3, 2017).

47. *See generally* Shaun Walker, *Face recognition app taking Russia by storm may bring end to public anonymity*, THE GUARDIAN (May 17, 2016), https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte [https://perma.cc/H3TG-TPQM] (touting the facial recognition technology, FindFace founder stated: "If you see someone you like, you can photograph them, find their identity, and then send them a friend request . . . It also looks for similar people. So you could just upload a photo of a movie star you like, or your ex, and then find 10 girls who look similar to her and send them messages").

48. Clay Dillow, *Augmented Identity App Helps You Identify Strangers on the Street*, POPULAR SCIENCE (Feb. 23, 2010), http://www.popsci.com/technology/article/2010-02/augmented-identity-app-helps-you-identify-friend-perfect-strangers [https://perma.cc/LL4T-7VBN].

Perhaps the biggest privacy issue with facial recognition is that "[o]nce someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the Government buildings you enter, and the photos your friends post online."[49] In fact, a series of experiments conducted at Carnegie Mellon University objectively concluded that "[i]f an individual's face on the street can be identified using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her."[50]

Accordingly, another significant privacy implication stems from the fact that "[o]nce data resides on the Internet, it is very difficult or impossible to erase."[51] This is because "[f]irms routinely take snapshots of the Internet that yield the cached webpages that turn up on your browser searches."[52] Even assuming that a person acted preemptively to try and protect their privacy online, the prevalence of data hacking presents a serious concern, especially in the wake of increased facial recognition technology use. For instance, in a 2013 cyber-attack, 1 billion Yahoo accounts were hacked, resulting in a data breach consisting of "sensitive user information, including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password."[53] Although the significance of Yahoo's data breach cannot not be discounted, the consequences and repercussions could have been much more severe had facial recognition data been involved, because "[y]ou can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face."[54]

---

49. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong 1–2 (2012) [hereinafter *Facial Recognition Hearing*] (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law), https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf [https://perma.cc/DT2B-KN5N].

50. *Id.* (testimony of Professor Alessandro Acquisti from Carnegie Mellon University), https://www.judiciary.senate.gov/imo/media/doc/12-7-18AcquistiTestimony.pdf [https://perma.cc/J2FM-AXCN].

51. MacLean, *supra* note 12, at 49.

52. *Id.* (citing Bernard J. Jansen et al., *Real Life, Real Users, and Real Needs: A Study and Analysis of User Queries on the Web*, 36 INFO. PROCESSING & MGMT. 207, 207 (2000)).

53. Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/6NP7-N3RL].

54. *Facial Recognition Hearing*, *supra* note 49, at 1 (opening statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

C. *Facebook's Current Capabilities with Facial Recognition Technology*

Facebook currently employs facial recognition technology to help users "tag"[55] friends in photos uploaded to the platform.[56] Although Facebook originally required users to manually tag friends, the company debuted "tag suggestions" in 2010 to make the tagging process easier for users.[57] Facebook describes its tag suggestions to users as follows: "When someone uploads a photo of you, we might suggest that they tag you in it. We're able to compare your friend's photos to information we've put together from your profile pictures and the other photos you're tagged in."[58] Facebook's final step is to then "associate the tags with your account, compare what these photos have in common and store a summary of this comparison."[59]

At the heart of tag suggestions is facial recognition technology. Mentioned briefly in Facebook's Help Center, the company's "facial recognition software [ ] uses an algorithm to calculate a unique number ('template') based on someone's facial features, like the distance between the eyes, nose and ears."[60] The template is crafted through a series of each user's profile pictures and tagged photos.[61] Although users can elect to disable the tag suggestion feature, meaning that Facebook will not suggest that people "tag you in photos that look like you,"[62] the company may still create a template using the individual user's profile picture and individually uploaded photos.[63]

Facebook's facial recognition technology enables the company to identify a person's face with nearly 98% accuracy.[64] Moreover, Facebook touts the fact that it can recognize and identify an individual in a single picture out of 800 million in under five seconds.[65] Unsurprisingly, "[d]ue to the large number of Facebook users and the fact that these users actively tag each other

55. According to Facebook, "[w]hen you tag someone, you create a link to their profile . . . [effectively] you can tag a photo to show who's in the photo." *What is tagging and how does it work?*, FACEBOOK, https://www.facebook.com/help/124970597582337 [https://perma.cc/DP5W-M62Q] (accessed Jan. 19, 2016).

56. *See generally Tagging Photos*, FACEBOOK, https://www.facebook.com/help/463455293673370 [https://perma.cc/GAV3-CQYH] (accessed Jan. 19, 2016).

57. *See generally Making Photo Tagging Easier*, FACEBOOK, https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/ [https://perma.cc/FS3Z-VQVW] (accessed Jan. 19, 2016).

58. FACEBOOK *supra* note 56, (accessed Jan. 19, 2016).

59. *Id*.

60. *Id*.

61. *Id*.

62. *Id*.

63. *Id*.

64. *See* Stacey Higginbotham, *Inside Facebook's Biggest Artificial Intelligence Project Ever*, FORTUNE (Apr. 13, 2016), http://fortune.com/facebook-machine-learning/ [https://perma.cc/E7FW-QGHN].

65. *Id*.

and themselves in photos, Facebook's face recognition system is the most robust and well-developed of all of these private sector products."[66]

It should be noted that Facebook's Data Policy allows users to access its "Download Your Information" tool.[67] However, the tool only yields a fractional portion of a user's personal data file, offering an arguably inadequate amount of information as to the biometric data that Facebook has on file for each particular user.[68] Figure A illustrates the entirety of information provided to inquiring users curious about the facial recognition data that Facebook has on file.[69]

Biz Carson

Facial Recognition Data

Threshold 1	3.5095708370209
Threshold 2	3.2094926834106
Threshold 3	1.668349981308
Example Count	237

Figure A [70]

A user proactively trying to discern what biometric data Facebook has stored on file would be presented with the nonsensical strand of numbers above in Figure A. An exhaustive search through Facebook's Help Center provides no explanation as to what "Thresholds 1, 2, 3" or "Example Count" refers, nor does Facebook include an explanation as to what facial recognition data the company actually has.[71] As such, while a user can technically view the facial recognition data that Facebook has stored, no meaningful information is actually provided.

66. Lynch, *supra* note 10, at 9.

67. FACEBOOK, *Accessing Your Facebook Data*, https://www.facebook.com/help/405183566203254/ (accessed Jan. 22, 2017) [https://perma.cc/2RJN-R7FW].

68. *Id*. ("We store different categories of data for different time periods, so you may not find all of your data since you joined Facebook"); *see also* Consumer Reports, *Facebook & your privacy: Who sees the data you share on the biggest social network?*, CONSUMER REPORTS MAGAZINE (June 2012), https://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm [https://perma.cc/6VN2-47BD].

69. Facebook's Download Your Information tool says that it provides users with Facial Recognition Data, which is "[a] unique number based on a comparison of the photos you're tagged in. We use this data to help others tag you in photos." However, the company does not explain the information downloaded as exemplified in Figure B. *See Accessing Your Facebook Data*, *supra* note 67.

70. Biz Carson, *I downloaded my data from Facebook and found all of the people I unfriended in the last 10 years*, BUSINESS INSIDER (May 19, 2016), http://www.businessinsider.com/how-to-download-data-from-facebook-2016-5/#in-the-settings-menu-where-you-normally-change-your-password-click-the-download-a-copy-button-2 [https://perma.cc/48DU-DEKT].

71. *Id*. ("Facebook even has my 'Facial Recognition Data' on file. The three thresholds mean nothing to me, but apparently Facebook has 237 examples of what I look like on file.").

The problem is that with no biometric privacy law on point, Facebook is operating unrestrained in its collection of its users face prints. Acting purely in the best interest of the company, Facebook issues its extraordinarily overbroad Terms of Service and Data Policy to its users, thereby granting the company an unprecedented level of freedom with respect to its data collection. The next section will demonstrate how Facebook's Terms of Service and Data Policy are unconscionable under California law due to the company's utilization of facial recognition technology and biometric data collection practices.

III. FACEBOOK FAILS TO EXPLICITLY INFORM CONSUMERS OF ITS USE OF FACIAL RECOGNITION TECHNOLOGY: HOW THE COMPANY'S TERMS OF SERVICE AND DATA POLICY SATISFY THE CALIFORNIA STANDARD FOR UNCONSCIONABILITY

A. The Doctrine of Unconscionability Under California Law

Notwithstanding the absence of a precise definition of unconscionability, several cases adjudicated in California[72] have adhered to the guidance set forth in *Williams v. Walker-Thomas*, which states: "Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party."[73] Accordingly, it is well-established that "the doctrine of unconscionability has both a procedural and a substantive element, the former focusing on oppression or surprise due to unequal bargaining power, the latter on overly harsh or one-sided results."[74]

For a contract to be rendered unconscionable, the party opposing the contract is required to show both procedural and substantive unconscionability.[75] However, California employs a "sliding scale" test, meaning that "the more substantively oppressive the contract term, the less evidence of procedural unconscionability is required to come to the conclusion that the term is unenforceable."[76]

---

72. *See, e.g.*, A & M Produce Co. v. FMC Corp., 135 Cal. App. 3d 473, 486 (4th Cir. 1982); Stirlen v. Supercuts, Inc., 51 Cal. App. 4th 1519, 1542 (Cal. App. 4th 1997); Dean Witter Reynolds v. Superior Court, 211 Cal. App. 3d 758, 767 (Cal. App. 3d 1989).

73. Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (D.C. Cir. 1965).

74. Sonic-Calabasas A, Inc. v. Moreno, 57 Cal. 4th 1109, 1133 (Cal. 2013); *see also* Baltazar v. Forever 21, Inc., 62 Cal. 4th 1237, 1233 (Cal. 2016); *A & M Produce Co.*, 135 Cal. App. 3d at 486.

75. *See* MATTHEW BENDER, CALIFORNIA CONTRACT LITIGATION, CH. 18, 18.15[3] (LEXIS 2016).

76. Armendariz v. Foundation Health Psychcare Services Inc., 24 Cal. 4th 83, 114 (Cal. 2000); *see also* Carboni v. Arropside, 2 Cal. App. 4th 76, 86 (Cal. Ct. App. 1991) (citing West v. Henderson, 227 Cal. App. 3d 1578, 1588 (Cal. App. 3d. 1991) (lending support to the fact that several California courts have acknowledged that "a compelling showing of substantive unconscionability may overcome a weaker showing of procedural unconscionability").

Pursuant to the California Civil Code, to properly assert this defense a contract or provision must "have been unconscionable at the time it was made."[77] In determining whether a contract or term is unconscionable, the "basic test is whether, in the light of the general commercial background and the commercial needs of the particular trade or case, the clauses involved are so one-sided as to be unconscionable under the circumstances existing at the time of the making of the contract."[78] Although unconscionability is more frequently litigated in situations where a contract contains an arbitration clause,[79] California courts have noted that the "unconscionability standard is, as it must be, the same for arbitration and nonarbitration agreements."[80]

In the commentary to California's unconscionability statute, the California Civil Code specifies that "[s]ection 1670.5 is intended to make it possible for the courts to police explicitly against the contracts or clauses which they find to be unconscionable."[81] Accordingly, California courts are seemingly both empowered and constrained by the lack of a precise definition of unconscionability, as they have free rein to define and apply the doctrine of unconscionability on a case-by-case context as they see fit, but are tasked with doing so without the assistance of formally defined rules and definitions.[82]

B. The Standard for Procedural Unconscionability

Procedural unconscionability is focused on "the manner in which the contract was negotiated and the circumstances of the parties at that time."[83] Specifically, this prong of the unconscionability doctrine is focused on the

77. Cal. Civ. Code § 1670.5(a) (2016).

78. *Id*. at cmt. 1.

79. *See generally*, Graham v. Scissor-Tail, Inc., 28 Cal. 3d 807 (Cal. 1981) (holding that a contract containing a mandatory arbitration clause was not unconscionable because it was within the plaintiff's reasonable expectations); Flores v. Transamerica HomeFirst, Inc., 93 Cal. App. 4th 846 (Cal. App. 4th 2001) (holding it unconscionable to include a mandatory arbitration clause in adhesion contract that is offered to consumers on a take-it-or-leave it basis).

80. Loewen v. Lyft, Inc., 129 F. Supp. 3d 945, 953 (N.D. Cal. 2015).

81. Cal. Civ. Code § 1670.5 cmt. 1 (2016) (comment 1 continues by explaining that "[i]n the past such policing has been accomplished by adverse construction of language, by manipulation of the rules of offer and acceptance or by determinations that the clause is contrary to public policy or to the dominant purpose of the contract.").

82. *See, e.g.*, Lewis A. Kornhauser, *Unconscionability in Standard Forms*, 64 CAL. L. REV. 1151, 1156 (1976), http://scholarship.law.berkeley.edu/californialawreview/vol64/iss5/2 [https://perma.cc/9C4S-THSQ] ("[t]he legal concept of unconscionability should be expanded"); *see also* Lyra Haas, *The Endless Battleground: California's Continued Opposition To The Supreme Court's Federal Arbitration Act Jurisprudence*, 94 B.U. L. REV. 1419, 1420, 1452 (2014), http://www.bu.edu/bulawreview/files/2014/08/HAAS.pdf [https://perma.cc/86K2-36AT] ("California courts have . . . *demonstrate[ed] a tendency to interpret each possible exception broadly and each power narrowly, pursuing every line of reasoning until cut off by contradictory Supreme Court jurisprudence* . . . the [California Supreme Court] still considers unconscionability a valid argument.") (emphasis added).

83. Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1179 (E.D. Mo. 2004).

elements of "oppression and surprise."[84] Additionally, several California courts have found that the "use of a contract of adhesion establishes a minimal degree of procedural unconscionability . . .".[85] In making this latter determination, courts consider whether there was an absence of real negotiation and "an absence of meaningful choice,"[86] as well as "the extent to which the supposedly agreed-upon terms of the bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed terms."[87] The elements used by courts to determine the existence of procedural unconscionability in a contract are discussed respectively below.

1. First Consideration: Facebook's Terms of Service and Data Policy Constitute an Adhesion Contract

Several California courts have held that "[a] finding of a contract of adhesion is essentially a finding of procedural unconscionability."[88] Because the "[u]nconscionability analysis begins with an inquiry into whether the contract is one of adhesion,"[89] determining that Facebook's Terms of Service and Data Policy constitute an adhesion contract is fundamental to explaining why courts should find these agreements to be unconscionable under California law.

An adhesion contract is presented by way of a standardized agreement: a party with "superior bargaining strength"[90] prepares and presents the terms of the contract to the other party, who can then either accept or reject the terms.[91] Simplified, contracts offered on a take-it-or-leave-it basis are referred to as adhesion contracts, and consumers are given two choices: complete adherence or complete rejection.[92] Adhesion contacts offer advantages, such as simplifying business operations, increasing efficiency, and reducing expenses.[93] In fact, it can be said that these types of agreements "appear to be a necessary concomitant of a sophisticated, mass-consumption economy."[94] Although standardized agreements have become increasingly commonplace

84. *A & M Produce Co.*, 135 Cal. App. 3d at 486; Cal. Civ. Code § 1670.5 cmt. 1 (2016).
85. BENDER, *supra* note 75, at 18.15[4][a].
86. *A & M Produce Co.*, 135 Cal. App. 3d at 486 (quoting Williams, 350 F.2d at 449).
87. *Id*. (citation omitted).
88. Nagrampa v. MailCoups, Inc., 469 F.3d 1257, 1281 (9th Cir. 2006) (quoting *Flores*, 93 Cal. App. 4th at 853; *see* also Circuit City Stores, Inc. v. Adams, 279 F.3d 889, 893 (9th Cir. 2002).
89. *Armendariz*, 24 Cal. 4th at 113 (citing *Graham*, 28 Cal. 3d at 817–19)).
90. Graham, 28 Cal. 3d at 817.
91. *See* E. ALLEN FARNSWORTH, CONTRACTS, ASPEN PUBLISHERS, 286 (4th ed. 2004).
92. *Id*.
93. *Id*. at 285.
94. Richard Sybert, *Adhesion Theory in California: A Suggested Redefinition and its Application to Banking*, 11 LOYOLA L.A. L. REV. 297, 298 (1978), http://digitalcommons.lmu.edu/llr/vol11/iss2/8 [https://perma.cc/2D5N-G6N3].

in society today,[95] and despite carrying with them certain benefits,[96] "[d]angers are inherent in standardization."[97]

A determination that Facebook's Terms of Service and Data Policy constitutes an adhesion contract is only the beginning of the inquiry, because "[t]o describe a contract as adhesive in character is not to indicate its legal effect."[98] Rather, an adhesion contract is presumptively deemed to be enforceable in California[99] "unless certain other factors are present which, under established legal rules – legislative or judicial -- operate to render it otherwise."[100]

As set forth in the Restatement Second of Contracts, the "more standardized the agreement and the less a party may bargain meaningfully, the more susceptible the contract or a term will be to a claim of unconscionability."[101] Significantly, although "new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract."[102] Of the many well-established principles in contract law, "[m]utual manifestation of assent, whether by written or spoken word or by conduct, is the touchstone of contract."[103]

When creating a Facebook account, prospective users are prompted to fill in their first and last name, mobile number or email, password, date of birth, and gender.[104] A small message sits above the sizable green "Create Account" button, reading: "By clicking Create Account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS Notifications from Facebook and can opt out at any

---

95. *See, e.g.*, Neal v. State Farm Ins. Co., 188 Cal. App. 2d 690, 694 (Cal. Ct. App. 1961) ("[T]oday, the impact of these standardized contracts can hardly be exaggerated Most contracts which govern our daily lives are of a standardised character."); Sybert, *supra* note 94 ("The individual's contractual relations and the incidents of daily life are defined by standardized agreements presented to him or her as faits accomplish.").

96. *See Graham*, 28 Cal. 3d at 818, n.15 (citing Richard Sybert, *Adhesion Theory in California: A Suggested Redefinition and its Application to Banking*, 11 LOYOLA L.A.L. REV. 297, 297–98) (acknowledging the benefits to standardized contracts: "Through advance knowledge on the part of the enterprise offering the contract that its relationship with each individual consumer or offeree will be uniform, standard and fixed, the device of form contracts introduces a degree of efficiency, simplicity, and stability. When such contracts are used widely, the savings in cost and energy can be substantial. An additional benefit is that the goods and services which are covered by these contracts are put within the reach of the general public, whose sheer size might prohibit widespread distribution if the necessary contractual relationships had to be individualized. Transactional costs, and therefore the possible prices of these goods and services, are reduced. In short, form contracts appear to be a necessary concomitant of a sophisticated, mass-consumption economy. They have social and economic utility").

97. FARNSWORTH, *supra* note 91, at 286.

98. *See Graham*, 28 Cal. 3d at 819.

99. *Id*. at 819–20.

100. *Id*. at 820.

101. RESTATEMENT (SECOND) OF CONTRACTS §208 cmt. a (Am. Law. Inst. 1981).

102. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004).

103. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 29 (2d Cir. 2002).

104. *See generally Home*, FACEBOOK, https://www.facebook.com/ [https://perma.cc/RFR9-X7DR] (accessed Apr. 4, 2017).

time."[105] Users then have the opportunity to click and read Facebook's hyperlinked Terms of Service and Data Policy before consenting to the entirety of the company's legally binding terms.[106] At this point, the prospective user must choose either to wholly accept Facebook's Terms of Service and Data Policy or forego an account altogether.[107] Because the company compels users to "unambiguously manifest either assent or rejection prior to being given access to the product,"[108] Facebook's Terms of Service and Data Policy should therefore be viewed as establishing the necessary element of procedural unconscionability.

However, it is important to note that California courts have rejected arguments of procedural unconscionability in adhesion contracts where the complaining party has a reasonable market alternative.[109] Additionally, the fact that a contract is one of adhesion does not automatically render it unconscionable, especially if there is no element of surprise included in the contract and its formation.[110] Each of these additional elements is discussed respectively below.

2. Second Consideration: Facebook's Terms of Service and Data Policy Are Imposed on Consumers in an Oppressive Manner

In a procedural unconscionability analysis, "'[o]ppression' arises from an inequality of bargaining power which results in no real negotiation and 'an absence of meaningful choice.'"[111] The inequality of bargaining power to the contract is best illustrated by *Ting v. AT&T*. In the case, AT&T mass mailed a Consumer Services Agreement ("CSA") containing a binding arbitration clause to over 60 million customers.[112] Prior to this mass mailing, AT&T issued a "market study [that] concluded that most customers 'would stop reading and discard the letter' after reading [a] disclaimer [stating]: . . . '[P]lease be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to

105. *Id.*

106. Referred to as the Statement of Rights and Responsibilities, users are told: "By using or accessing the Facebook Services, you agree to this Statement, as updated from time to time in accordance with Section 13 below." *Terms of Service*, FACEBOOK, (last revised Jan. 30, 2015), https://www.facebook.com/legal/terms [https://perma.cc/5YFP-9CEW] (accessed Apr. 4, 2017).

107. *Id*.

108. *Register.com, Inc.*, 356 F.3d at 429.

109. *Dean Witter Reynolds*, 211 Cal. App. 3d at 769–72 ("Even though a contract may be adhesive, the existence of 'meaningful' alternatives available to such contracting party in the form of other sources of supply tends to defeat any claim of unconscionability as to the contract in issue."); *Cf.* Gatton v. T-Mobile USA, Inc., 152 Cal. 4th 571, 585 (Cal. 4th 2007) (noting that the existence or availability of market alternatives does not preclude a finding that an adhesion contract is sufficient to establish some level of procedural unconscionability).

110. FARNSWORTH, *supra* note 91, at 302.

111. *A & M Produce Co.*, 135 Cal. App. 3d at 486 (quoting *Williams*, 350 F.2d at 449).

112. *See* Ting v. AT&T, 319 F.3d 1126, 1133–34 (9th Cir. 2003).

do.'"[113] The agreement stated that customers would assent to the terms "by continuing to use or to pay for AT&T's service."[114] The *Ting* Court held the CSA to be procedurally unconscionable because "AT&T imposed the CSA on its customers without opportunity for negotiation, modification, or waiver" and "offered its terms on a take-it-or-leave-it basis."[115]

a. *Consumers Have an Indisputable Inequality in Bargaining Power*

In the same vein as *Ting*, Facebook users have no meaningful opportunity to negotiate with the company. If a Facebook user has even a single concern or reservation about a term included in the Terms of Service or Data Policy, that user's only option is to forego use of the platform entirely or otherwise succumb to each and every one of Facebook's terms.[116] As in *Ting*, solely considering the lack of bargaining power and the fact that Facebook offers its terms to users strictly on a take-it-or-leave-it basis, there is at least some element of procedural unconscionability present in Facebook's Terms of Service and Data Policy.[117]

b. *Consumers Have a Lack of Meaningful Choice In Controlling Their Biometric Data, Obtained Non-Consensually by Facebook*

The lack of meaningful choice for consumers with respect to the inclusion of facial recognition data in Facebook's Terms of Service and Data Policy is highlighted by the fact Facebook provides no publicly available information regarding how long the company will retain its users biometric identifiers.[118] More troubling is that Facebook offers neither instruction nor choice for users to permanently destroy any biometric identifiers collected by the company.[119] This lack of choice and bargaining power is imperative

113. *Id*. at 1134.
114. *Id*.
115. *Id*. at 1149.
116. *See Terms of Service*, *supra* note 106 ("By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use. You may receive SMS Notifications from Facebook and can opt out at any time", offering no alternative contact information for users concerned with the company's Terms and Data Policy).
117. *Id*.
118. *See* Patel v. Facebook, Inc., No. 1:15-CV-04265, 2015 WL 2265958, ¶ 20 (N.D. Ill. May 14, 2015) (discussing "Facebook's failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of its users' biometric information").
119. Although users can elect to delete their Facebook accounts, there is a 14-day window before deletion takes effect. Moreover, in its Help Center, Facebook reserves the right to keep any account data for up to 90 days after deletion (https://www.facebook.com/help/125338004213029). For a more in-depth discussion on how Facebook has been criticized for making the deletion process deceptively difficult for users, *see generally* Glenn Stok, *Facebook's Deception of Deactivated Accounts*, TURBOFUTURE (last

because "[b]iometrics [] are biologically unique to the individual; therefore, once compromised, the individual has no recourse."[120] Even after a user manually opts-out of biometric data collection, Facebook still retains the previously collected data, regardless of whether or not the user consented to collection in the first place.[121] In fact, Facebook's full Data Policy states that even after a user deletes his or her account, the company "store[s] data for as long as it is necessary to provide products and services to [] others."[122] This clause offers neither precise information for users as to a retention timetable nor guidelines for permanent destruction of data.[123] The risk of harm here is that Facebook is already in the business of profiting off consumer data,[124] and with no meaningful choice for users to completely and unquestionably opt-out of biometric data collection, and no transparency as to if and when Facebook will truly remove such data, users are left in the dark.

Although Facebook states that a user can disable the Tag Suggestions feature and manually opt-out of being included in the facial recognition database, [125] this is somewhat misleading and easily susceptible to varying interpretations. On numerous occasions, Facebook has publicly announced that if a user disables tag suggestions, then despite "if a facial recognition template was created, it will be deleted," whether from tagged photos or profile pictures.[126] However, in Facebook's Help Center it states that "[w]hen

---

updated Mar. 26, 2017), https://turbofuture.com/internet/Obsolete-Facebook-Profile-Charade [https://perma.cc/RFM9-7PVJ].

120. *See* S. 95-2400, 2nd Sess., at 1 (Ill. 2008).

121. *See Data Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy [https://perma.cc/MJS4-8Y2W] (accessed Jan. 22, 2017); *see also Facial Recognition Hearing*, *supra* note 49, at 2 (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

122. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ [https://perma.cc/4S7T-MCEM] (last modified Sept. 16, 2016).

123. Facebook is currently being sued by Illinois users under the Illinois Biometric Privacy Information Act in the U.S. District Court for the Northern District of California. The plaintiffs are alleging, among other claims, that the company failed to "provide a publicly available retention schedule and guidelines for permanently destroying the biometric identifiers of plaintiffs and the class (who do not opt-out of 'Tag Suggestions')". *See* In Re Facebook Biometric Information Privacy Litigation, Case No. 15-cv-03747-JD (N.D. Cal. 2016).

124. *See generally* Jason Kint, *Google and Facebook devour the ad and data pie. Scraps for everyone else*, DIGITAL CONTENT NEXT (June 16, 2016), https://digitalcontentnext.org/blog/2016/06/16/google-and-facebook-devour-the-ad-and-data-pie-scraps-for-everyone-else/ [https://perma.cc/6Q75-8VYJ].

125. *See How does Facebook suggest tags?*, FACEBOOK HELP CENTER , https://www.facebook.com/help/122175507864081?helpref=faq_content [https://perma.cc/7SCS-DVAN] (last visited Apr. 3, 2017) ("If you remove a tag from a photo, that photo is not used to create the template for person whose tag was removed.").

126. *Facial Recognition Hearing*, *supra* note 49, at 29 (statement of Richard Sherman, Manager of Privacy & Public Policy at Facebook); *see also* Alexei Oreskovic, *Facebook may add your profile photo to facial recognition database*, NBC NEWS (Aug. 29, 2013 12:23 PM), http://www.nbcnews.com/technology/facebook-may-add-your-profile-photo-facial-recognition-database-8C11030921 [https://perma.cc/FUC7-LFAP] (noting that Facebook Chief Privacy Officer Erin Egan "stressed that Facebook users uncomfortable with facial recognition technology will still be able to 'opt out' of the Tag Suggest feature altogether, in

you're tagged in a photo, or make a photo your profile picture, we associate the tags with your account, compare what these photos have in common and store a summary of this comparison," offering no indication or guarantee that any associated facial recognition data obtained from the user's profile pictures will subsequently be deleted after a user disables Tag Suggestions.[127] In fact, it seems that disabling Tag Suggestion simply removes the option for Facebook to suggest that one user tags another user in a photo. Ultimately, even if a user turns off Tag Suggestions, Facebook may still retain a summary template of that user's facial data from his or her pictures.[128] As such, users have no choice regarding if or how Facebook stores their biometric data: users simply have to sign away their right to control their biometric data or forego using the platform altogether.

Perhaps more troubling is that Facebook began collecting face prints prior to obtaining explicit consent from its users to do so, meaning that users were never initially given a choice on whether or not they wanted Facebook to start collecting their face prints. Facebook began collecting data from user-uploaded photographs in order to develop its robust facial recognition data library without knowledge or consent from its billion-plus account holders.[129] After initially announcing the creation of Tag Suggestions, Facebook hastily publicized that the feature had actually already been deployed both domestically and internationally, absent any notice or consent from its users.[130] Only after coming under fire did Facebook admit that it "should have been more clear with people during the roll-out process when this became available to them."[131] Simply put, not only were users blatantly unaware that Facebook was going to begin using facial recognition technology, but users had no meaningful choice to affirmatively opt-out of this invasive biometric data collection, because Facebook automatically opted-in all users.[132] Thus,

---

which case the person's public profile photo would not be included in the facial recognition database.").

127. *See generally* FACEBOOK HELP CENTER, https://www.facebook.com/help/218540514842030?helpref=faq_content [https://perma.cc/R6Z5-Q93K]; *See also How does Facebook suggest tags?*, FACEBOOK, https://www.facebook.com/help/122175507864081?helpref=faq_content [https://perma.cc/8P2K-H9M2] (accessed Apr. 3, 2017).

128. *Id*.; *see also* Lynch, *supra* note 10, at 10 ("even if a user deletes the summary data, it is unclear whether taking this step will prevent Facebook from continuing to collect biometric data going forward.").

129. *See* ELECTRONIC PRIVACY INFORMATION CENTER, IN THE MATTER OF FACEBOOK, INC. AND THE FACIAL IDENTIFICATION OF USERS, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission, 10–11 (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [https://perma.cc/6BAU-NKM7].

130. *Id*. at 10 (citation omitted).

131. *See* ELECTRONIC PRIVACY INFORMATION CENTER, IN THE MATTER OF FACEBOOK, INC. AND THE FACIAL IDENTIFICATION OF USERS, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission, 11 (June 10, 2011), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [https://perma.cc/6BAU-NKM7].

132. *Facial Recognition Hearing*, *supra* note 49, at 2 (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

without notice, Facebook automatically enabled the facial recognition feature to its unsuspecting, non-consenting 500 million users in 2011.[133]

Facebook's lack of notice and transparency regarding its stealth and non-consensual deployment of facial recognition technology became the focal point of a 2012 Senate Subcommittee on Privacy, Technology and the Law hearing, in which Senator Al Franken asked Facebook's Privacy and Policy Manager the obvious question: "How can users make an informed decision about facial recognition in their privacy settings if you don't actually tell them that you are using facial recognition?"[134] Further, when asked whether the company would ever sell its facial recognition data and information to third parties, Facebook's Privacy and Policy Manager offered no guarantees, eerily remarking that "[i]t's difficult to know what Facebook will look like five or 10 years down the line, so it's hard to respond to that."[135] Yet six years later, in 2018, Facebook is still programmed to automatically opt-in users to its biometric data collection upon sign-up, absent any notice of this practice in the company's Terms of Service and Data Policy. Considering the above factors, courts should view the unreasonable lack of meaningful choice for consumers with respect to Facebook's biometric data collection practices as supporting evidence in finding procedural unconscionability.

c. *Practically Speaking, No Other Social Media Platforms Are Comparable as a Meaningful Alternative to Facebook*

It is true that some California courts have held that "[t]here can be no oppression establishing procedural unconscionability, even assuming unequal bargaining power and an adhesion contract, when the customer has meaningful choices."[136] But in this day and age, from a purely statistical standpoint, there really is not a meaningful alternative to Facebook. This is best evidenced by a 2016 Pew Research Center study that showed that Facebook is still the most popular and widely used social networking platform by a "substantial margin," with eight out of 10 Americans, or 79% of all Internet users, using the platform.[137] Instagram falls in second place, with a

133. *See* Charles Arthur, *Facebook in new privacy row over facial recognition feature*, THE GUARDIAN (June 8, 2011), https://www.theguardian.com/technology/2011/jun/08/facebook-privacy-facial-recognition [https://perma.cc/56HN-2NPD].

134. Ricardo Bilton, *Facebook hit with tough questions on facial recognition in Senate hearing*, VENTUREBEAT (July 18, 2012), http://venturebeat.com/2012/07/18/facebook-hit-with-tough-questions-on-facial-recognition-in-senate-hearing/ [https://perma.cc/manage/create].

135. *Id*.

136. Wayne v. Staples, Inc., 135 Cal. App. 4th 466, 482 (Cal. App. 2d 2006); *see also Dean Witter Reynolds*, 211 Cal. App. 3d at 771.

137. *See* Shannon Greenwood, et al., *Social Media Update 2016*, PEW RESEARCH CENTER (Nov. 11, 2016), http://www.pewinternet.org/2016/11/11/social-media-update-2016/ [https://perma.cc/N6VM-BP6M].

mere 32% of Americans using the photo hosting platform.[138] The enormous disparity in users of each respective platform cannot be overstated, especially when comparing Facebook's 1.86 billion[139] daily active users to Instagram's 600 million[140] daily active users.

At first blush, it may seem as though Instagram provides a meaningful alternative to Facebook. However, Facebook actually owns its second-place rival Instagram. According to Instagram's Privacy Policy, the company has "collaborat[ed] with Facebook's team . . . to share insights and information with each other" since 2013.[141] In an effort to discern just how much information the two companies share, a reporter from The Wall Street Journal "created a fresh Instagram account with [her] work email and didn't sync it to Facebook . . . [finding that] 78 out of 100 [of Instagram's follower] recommendations were [her] Facebook friends."[142] This happened because "[e]ven when [users] don't upload [their] contacts directly to Instagram, the network uses information—or 'signals,' as Instagram calls them—from Facebook, which might include contacts or other tangential information."[143] Thus, even if consumers opted to use Instagram as an alternative to Facebook, Facebook would still be in total control of consumer information as the company "share[s] information about [consumers] within [its] family of companies."[144] For users seeking to distance themselves from Facebook's onerous Terms of Service and Data Policy, a Facebook-owned company simply cannot be considered a meaningful alternative to Facebook.

As such, a consumer hoping to stay socially engaged while bypassing Facebook's family of companies and their corresponding overreaching terms could turn to Twitter, the third most used social media site.[145] But with only 21% of the United States' adult population using Twitter, the application hardly stands as a meaningful alternative to Facebook.[146] In fact, it has been noted that "[p]opular digital monopolies, such as Google, Facebook, or Microsoft, *offer no free choice* compared to alternative services, which could be of inferior quality, be it because they are as yet under-developed or less

138. *Id*.

139. FACEBOOK, *supra* note 13.

140. *See generally* INSTAGRAM, http://blog.instagram.com/post/154506585127/161215-600million [https://perma.cc/B9NX-6AAS] (accessed Jan. 19, 2016).

141. *See generally* INSTAGRAM, https://help.instagram.com/155833707900388 [https://perma.cc/R6QH-XCXT] (accessed Feb. 13, 2018).

142. Katherine Bindley, *Instagram is Turning Into Facebook, And That's Bad*, WALL ST. J. (Feb. 13, 2018), https://www.wsj.com/articles/instagram-is-turning-into-facebook-and-thats-bad-1517422670.

143. *Id*.

144. *See generally The Facebook Companies*, FACEBOOK, https://www.facebook.com/help/111814505650678 [https://perma.cc/49NY-HEUK] (accessed Apr. 6, 2017).

145. Greenwood, et al., *supra* note 137.

146. *Id*.

innovative or be it that they are so because such services do not process significant data from their users."[147]

Aside from Facebook's proven and significant half-billion user advantage over its competitors, the demographics of Facebook's users bolster the argument that no other social networking platform provides a similar alternative to Facebook. To illustrate, studies have shown that 64% of all online Americans said the motivation for using social networking sites was to keep in touch with family members,[148] a sentiment that especially rings true for the baby boomer generation and beyond.[149] As such, it cannot be overlooked that while 62% of adults aged 65+ use Facebook, only a mere 8% of the 65+ population use Instagram.[150]

These numbers undoubtedly show that Facebook is the most commonly utilized social networking tool for Americans, ranging from teenagers to senior citizens. If social media is truly used to keep in touch with family members, then Facebook is the sole platform that makes this feasible. In other words, although there are a variety of other social networking platforms, none offer Facebook's cross-generational reach.

Of course, there is the argument that "if you don't like it, then don't use it."[151] However, for better or for worse, social media has engrained itself in

147. Anca D. Chirita, *The Rise of Big Data and the Loss of Privacy*, Durham Law School Research Paper, 10 (June 15, 2016), https://ssrn.com/abstract=2795992 [https://perma.cc/8QX4-N6MT] (emphasis added).

148. *See* Aaron Smith, *Why Americans use social media*, PEW RESEARCH CENTER (Nov. 15, 2011), http://www.pewinternet.org/2011/11/15/why-americans-use-social-media/ [https://perma.cc/K838-UJ84].

149. *See* Nora Krug, *Technology helping more baby-boomer grandparents stay plugged in to grandkids*, WASH. POST (Oct. 31, 2014) (accessed Jan. 19, 2016), https://www.washingtonpost.com/postlive/technology-helping-more-baby-boomer-grandparents-stay-plugged-in-to-grandkids/2014/10/31/3dda3c26-4ccb-11e4-aa5e-7153e466a02d_story.html?utm_term=.71c3d6bb6743 [https://perma.cc/JV8P-LZPN]. For example, Facebook provides a useful platform for families to stay in touch and for grandparents to be involved in the lives of their grandchildren. With the median household income in the U.S. clocking in at $56,516. *See* Bernadette D. Proctor et al., *Income and Poverty in the United States: 2015*, U.S. CENSUS BUREAU, Report Number: P60-256 (Sept. 13, 2016), http://www.census.gov/library/publications/2016/demo/p60-256.html) [https://perma.cc/4N7C-DGVZ], and average round-trip domestic airfare costs around roughly $400 per person (*see* U.S. Dep't of Transp., Bureau of Transportation Statistics (2015), https://www.rita.dot.gov/bts/airfares/programs/economics_and_finance/air_travel_price_index/html/AnnualFares.html [https://perma.cc/27PH-Y4QL]), traveling to see family and friends in other states can be costly and difficulty. In fact, a 2012 AARP study revealed that 67% of grandparents who reported infrequent visits with their grandchildren cited distance as the reason why (Cheryl L. Lampkin, PhD, *Insights and Spending Habits of Modern Grandparents*, AARP (Sept. 5, 2012), http://www.aarp.org/research/topics/life/info-2014/grandparenting-survey.html [https://perma.cc/JS6X-4G9G]).

150. Greenwood, et al., *supra* note 137.

151. *See, e.g.*, *"If you don't like it, don't use it. It's that simple." ORLY?*, SOCIAL MEDIA COLLECTIVE, (Aug. 11, 2011), https://socialmediacollective.org/2011/08/11/if-you-dont-like-it-dont-use-it-its-that-simple-orly/ [https://perma.cc/K5WV-WC8U] ("It's common, and easy, to say 'just don't use it.' There's actually a term for this– technology refusal– meaning people who strategically 'opt out' of using overwhelmingly prevalent technologies . . . [but] 'if you don't like it, don't use it' is not really simple at all.").

our society as a necessity of sorts, rapidly losing any semblance of voluntariness. [152] As indicated by the statistics above, there is arguably no meaningful alternative for consumers, as Facebook has taken a clear and decisive lead over its competitors.

This lack of meaningful choice was recognized as far back as 2010 in a New York Times article which stated: "In reality, quitting Facebook is much more problematic than the company's executives suggest, if only because users cannot extract all the intangible social capital they have generated on the site and export it elsewhere."[153] As a result, "many users find it too daunting to start afresh on a new site, so they quietly consent to Facebook's privacy bullying."[154]

The bare existence of other social media platforms does not satisfy the element of a meaningful alternative. It is well-established under California law that a "claim of procedural unconscionability cannot be defeated merely by 'any showing of competition in the marketplace as to the desired goods and services . . . ".[155] As the most utilized platform across the spectrum that is statistically and objectively proven to saturate the market, Facebook should not put its users in a position to make a value judgment between staying connected or sacrificing their privacy.

3. Third Consideration: By Explicitly Omitting Mention of Facial Recognition Technology in its Terms of Service and Data Policy, Facebook's Policies Contain a Surprise for Consumers

In a procedural unconscionability analysis, "surprise involves the extent to which the supposedly agreed-upon terms of the bargain are hidden in a

152. *See, e.g.*, Lynch, *supra* note 10, at 3 ("Americans cannot participate in society without exposing their faces to public view. Similarly, connecting with friends, family and the broader world through *social media has quickly become a daily (and some would say necessary) experience for Americans of all ages*") emphasis added; *see also* SOCIAL MEDIA COLLECTIVE, *supra* note 151 (the leading comment on this article from user Steve Boland reads: "I did leave Facebook in a self-righteous huff, having had enough of how they treat their customers. I took the 'Don't like Facebook? Leave Facebook.' approach. Then I came crawling back, six months later. I was socially isolated. It was too difficult to keep [up] with [] people when I couldn't be reached as easily as other family and friends. The cost of not participating in the free service was too high"); *see also* Nicole B. Ellison, et al., *The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites*, 12 Journal of Computer-Mediated Communication 1143, 1164 Mich. St. U. 2007 (http://www.michelepolak.com/200fall11/Weekly_Schedule_files/Ellison.pdf) [https://perma.cc/NDN8-3HET] (research study illustrating Facebook's edge in cultivating friendship, concluding that "Internet use alone did not predict social capital accumulation, but intensive use of Facebook did.").

153. Evgeny Morozov, *Surfing the Surfer*, NY Times (June 1, 2010), http://www.nytimes.com/2010/06/02/opinion/02iht-edmorozov.html [https://perma.cc/96ZV-9NY5].

154. *Id*.

155. Comb v. Paypal, Inc., 218 F. Supp. 2d 1165, 1173 (N.D. Cal. 2002) (quoting *Dean Witter Reynolds*, 211 Cal. App. 3d at 772.

prolix printed form drafted by the party seeking to enforce the disputed terms."[156] The element of surprise is generally focused on the terms included in the agreement at issue.[157] Nowhere in Facebook's Terms of Service or Data Policy is the phrase "facial recognition technology" explicitly used.[158] Yet, upon careful review, facial recognition data collection from photos is assumedly included under what Facebook refers to as "IP Content,"[159] termed by Facebook to include things "like photos and videos."[160] In other words, users would need to be specifically searching on Facebook's Help Center, which is wholly separate from the company's Terms of Service or Data Policy, to find any information about the company's use of facial recognition technology.[161] Yet when signing up for the platform, users are prompted that by signing up they "agree to [the] Terms and that [they] have read [Facebook's] Data Policy,"[162] neither of which include the term facial recognition nor a description of how Facebook collects and uses that technology.[163] The problem, then, is that users consent to the Terms of Service and Data Policy – not to the Help Center – meaning that they simply cannot agree to something that is not there.

By tactfully omitting the term "facial recognition technology" from its Terms of Service and Data Policy, Facebook is taking advantage of unsuspecting users who simply do not know what they do not know.[164] Considering that the element of surprise in an unconscionability determination concerns whether certain terms are concealed or buried within the contract,[165] the omission of any reference to facial recognition technology is wholly significant. Facebook did not merely hide its right to collect and use facial recognition data in a shuffle of other terms in hopes that its users would not read the Terms of Service and Data Policy. Rather, the company flat-out failed to include any reference to facial recognition technology in its Terms of Service and Data Policy – the two agreements to which users are required

156. *A & M Produce Co.*,135 Cal. App. 3d at 486.
157. *Id*.
158. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 122.
159. *Id*.
160. *Id*.
161. *See* https://www.facebook.com/help/122175507864081?helpref=faq_content for the lone search result for "facial recognition" on Facebook's Help Center (accessed Apr. 4, 2017).
162. Facebook home page, https://www.facebook.com/ (accessed Apr. 4, 2017).
163. *Id*.
164. *See* Yasamine Hashemi, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability,* 15 B.U. J SCI & TECH L. REV. 140, 158 (2009), https://www.bu.edu/jostl/files/2015/02/Hashemi_WEB_151.pdf (noting that "[t]here is evidence that most Facebook members do not read these documents in the first place . . . [which] could support an argument that they are unduly long and confusing, or that there is no possibility that they could bargain with Facebook to change the language into terms that are more member-friendly. This would support a finding of procedural unconscionability."). The author makes a strong argument that a user's failure to read Facebook's excessively lengthy terms could support a finding of procedural unconscionability.
165. *A & M Produce Co.*, 135 Cal. App. 3d at 486 (citing M.P. Ellinghaus, *In Defense of Unconscionability* 78 YALE L.J. 757, 764–765 (1969)).

to assent in order to use the platform.[166] As such, even if users read the entirety of Facebook's terms and policies, there is no explicit information on facial recognition technology to which users can even contemplate consenting.[167]

Another surprise term is found in Facebook's Terms of Service, outlining that users grant to the company "a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content" posted "on or in connection with Facebook."[168] Essentially, this clause in the Terms of Service allows Facebook, carte blanche, to collect, use, and share any and all content at the company's discretion, without any payment or notice of such use or distribution to the impacted users.[169] In practice, not only does Facebook fail to offer adequate notice to its users upon sign-up about the company's facial recognition practices, but Facebook then reserves for itself the an explicit license to any biometric data subsequently collected for an undetermined and undisclosed period of time.[170]

With this in mind, California courts should find the exclusion of facial recognition terminology in the Terms of Service and Data Policy, coupled with the company's exclusive license to use such data, as a contractual surprise, thereby making any use and licensure of biometric data unconscionable and subsequently void.

---

166. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 122 (providing no terminology or explanation regarding the company's practice of collecting and using facial recognition technology).

167. As of February 27, 2018, Facebook began issuing pop-up notices to some, not all, of its *existing* users, in which it described in very little detail the company's facial recognition practices. *See* Russell Brandom, *Facebook is starting to tell more users about facial recognition*, THE VERGE (Feb. 27, 2018), https://www.theverge.com/2018/2/27/17058268/facebook-facial-recognition-notification-opt-out. However, at the time of this note publication, Facebook still explicitly excludes any mention of facial recognition technology in its Terms of Service and Data Policy for *prospective* users. As a result, a prospective user would sign-up for Facebook with no notice of the company's facial recognition practices, and would subsequently be opted-in to Facebook's biometric data collection. Due to the sensitive nature of biometric data, it is simply not enough for Facebook to only notify *some* of its *existing* users about this technology: Facebook needs to provide explicit notice to its *prospective* users as well in either its Terms of Service or Data Policy.

168. *Terms of Service*, *supra* note 106.

169. *See* Oliver Smith, *Facebook terms and conditions: why you don't own your online life*, THE DAILY TELEGRAPH (Jan. 4, 2013), http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html ("Specifically for photos and video uploaded to the site, Facebook has a license to use your content in any way it sees fit, with a license that goes beyond merely covering the operation of the service in its current form. Facebook can transfer or sub-license its rights over a user's content to another company or organization if needed. Facebook's license does not end upon the deactivation or deletion of a user's account, content is only released from this license once all other users that have interacted with the content have also broken their ties with it.").

170. *See* Lynch, *supra* note 10, at 11 ("All of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large.").

a. *Merging Surprise with Failure to Read – How to Remedy and Address This Counterargument*

An important consideration is whether a user's failure to read terms and policies should be taken into consideration when asserting the defense of unconscionability.[171] The California Supreme Court has rejected "[t]he suggestion that a contract or clause cannot be unconscionable if it is accepted by a knowledgeable party."[172] Indeed, although there is commonly a duty and expectation to read a contract before assenting to it, California courts have recognized that "no authority is cited for a supposed rule that if a party reads an agreement he or she is barred from claiming it is unconscionable," adding that "[s]uch a rule would seriously undermine the unconscionability defense."[173]

Although, generally speaking, "'one who signs an instrument may not avoid the impact of its terms on the ground that he failed to read the instrument before signing it,'"[174] this general rule is applicable "only in the absence of 'overreaching'[175] or 'imposition.'"[176] In fact, failure to read a contract is actually deemed to be helpful in establishing "actual surprise."[177]

With respect to whether sufficient consent was given by a user who may or may not have read the terms, one expert in the area has said "[o]ne of the issues will be whether the consent was obtained under circumstances where people understand what they're agreeing to . . . [h]ow many times have you clicked through 'I consent' licenses on software and Web sites? I write those for a living, and I don't read them."[178] But even if a diligent user were to read the entirety of Facebook's terms and policies, there is no explicit information on facial recognition technology included therein to which the user could contemplate consenting.[179]

By failing to mention its use of facial recognition technology in its Terms of Service and Data Policy to prospective users, Facebook is collecting

171. For better or for worse, it is widely regarded that consumers often neither read nor understand the terms included in adhesion contracts. Instead, consumers misguidedly "trust to the good faith of the party using the form and to the tacit representation that like terms are being accepted regularly by others similarly situated." RESTATEMENT (SECOND) OF CONTRACTS, §211 cmt.b (Am. Law. Inst. 1981).

172. *Stirlen*, 51 Cal. App. 4th at 1534.

173. Higgins v. Superior Court, 140 Cal.App. 4th 1238, 1251 (Cal. App. 4th 2006).

174. Bruni v. Didion, 160 Cal. App. 4th 1272, 1291 (Cal. App. 4th 2008) (citation omitted).

175. *Bruni*, 160 Cal. App. 4th at 1291 (quoting Stewart v. Preston Pipeline Inc., 134 Cal.App. 4th 1565, 1588 (Cal. App. 4th 2005)).

176. *Bruni*, 160 Cal. App. 4th at 1291(quoting Jefferson v. Dep't of Youth Auth., 28 Cal. 4th 299, 303 (Cal. App. 4th 2002)).

177. *See Bruni*, 160 Cal. App. 4th at 1291 (quoting Patterson v. ITT Consumer Fin. Corp., 14 Cal.App. 4th 1659, 1666 (Cal. App. 4th 1993).

178. Caroline McCarthy, *Legally, are Facebook's Social ads Kosher?*, CNET NEWS (Nov. 15, 2007, 8:17 PM), http://www.news.com/8301-13577_3-9817421-36.html (quoting Brian Murphy, a partner at Frankfurt Kurnit Klein & Selz specializing in intellectual property issues and content licensure).

179. *See Terms of Service*, *supra* note 106.

biometric data wholly without consent.[180] This matters because "[f]acial recognition is one of those categories of data where a very prominent and a very clear consent is necessary."[181] Users cannot agree to something that is neither mentioned nor included in the terms presented, and in the case of Facebook's Terms of Service and Data policies, it is inconsequential whether or not a user reads or fails to read the terms and provisions because there is simply no mention of facial recognition technology whatsoever. The most careful reader would be unable to find mention of the term, meaning that there simply cannot be a failure to read when there is nothing in question to be read.[182]

Considering the adhesive nature of the contract, the unequal bargaining positions, the lack of meaningful choice, and the surprise, hidden contractual terms, it would be prudent for California courts to follow precedent and find that there is a sufficient showing of procedural unconscionability in Facebook's Terms of Service and Data Policy. The analysis would then turn to whether substantive unconscionability is also present.

C. The Standard for Substantive Unconscionability

Unlike procedural unconscionability, "[s]ubstantive unconscionability is less easily explained."[183] Substantive unconscionability often refers to an "allocation of risks or costs which is overly harsh or one-sided and is not justified by the circumstances in which the contract was made."[184] California courts are split as to the standard for substantive unconscionability: some require that substantive unconscionability rise to a level that "shock[s] the

180. Lynch, *supra* note 10, at 10 ("[I]t turned these features on by default. It first enrolled all its users in the system without prior consent and then continued to opt-in users every time they uploaded a photograph.").

181. Rachel Adams-Heard, *Facebook's Facial Recognition Software Draws Privacy Complaints, Lawsuit*, INSURANCE JOURNAL (July 30, 2015), http://www.insurancejournal.com/news/national/2015/07/30/376972.htm [https://perma.cc/6S9J-ZAZY] (quoting Alvaro Bedoya, executive director of Georgetown University's Center on Privacy & Technology).

182. Failure to read presents an interesting policy and moral question for California courts: should consumers be held liable for unconscionable adhesion contracts that they failed to read in full? In pondering this question, it is imperative to consider a July 2016 study which showed that, for the most part, users simply do not read Terms of Service Agreements and Privacy Policies. The experiment created a fictional social networking service and asked participants to read the Terms of Service Agreement and Privacy Policy. Aside from sharing all user data with the National Security Agency ("NSA") and the participant's employers, one of the clauses in the Terms of Service provided that participants would deliver their first-born child as payment for access to the social networking service. This sacrificial-child clause went unnoticed by 98% of the study's participants, with only 1.7% of the participants noticing and raising a concern with the clause. Jonathan A. Obar & Anne Oledorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, (Aug. 24, 2016), http://dx.doi.org/10.2139/ssrn.2757465.

183. *Stirlen*, 51 Cal. App. 4th at 1532.

184. Cal. Civ. Code § 1670.5 n.2 (2016); *see also A & M Produce Co.*, 135 Cal. App. 3d at 486; *Armendariz*, 24 Cal. 4th at 114.

conscience,"[185] while others require a less onerous showing of failure to act in "good faith and fair dealing."[186] Regardless, it is well-accepted that "a contractual term is substantively suspect if it reallocates the risks of the bargain in an objectively unreasonable or unexpected manner."[187]

In assessing substantive unconscionability, California courts often consider whether the contractual terms at issue "contravene the public interest or public policy,"[188] whether the questionable terms are included in the contract in "fine print,"[189] and whether the terms "seek to negate the reasonable expectations of the nondrafting party."[190] The Legislative Committee Comments to the California Civil Code on unconscionability state that courts can "police explicitly against the contracts or clauses which they find to be unconscionable" by examining whether the "clause is contrary to public policy or to the dominant purpose of the contract."[191]

Important to note, a showing of substantive unconscionability "requires a substantial degree of unfairness beyond 'a simple old-fashioned bad bargain.'"[192]

It is well understood by California courts that "[n]ot all one-sided contract provisions are unconscionable; hence the various intensifiers in [the California court] formulations: '*overly* harsh,' '*unduly* oppressive,' '*unreasonably* favorable.'"[193] As such, "[a] contract term is not substantively unconscionable when it merely gives one side a greater benefit."[194] Accordingly, as articulated in *Stirlen v. Supercuts, Inc.*, "a contract can provide a 'margin of safety' that provides the party with superior bargaining strength a type of extra protection for which it has a legitimate commercial need without being unconscionable." However, the *Stirlen* court clarified that "unless the 'business realities' that create the special need for such an advantage are explained in the contract itself [] [then] it must be factually established."[195]

185. *See* California Grocers Ass'n. v. Bank of Am., 22 Cal. App. 4th 205, 215 (Cal. Ct. App. 1994).

186. *See* Donovan v. Rrl Corp., 26 Cal. 4th 261, 290–91 (Cal. 2001).

187. *Stirlen*, 51 Cal. App. 4th at 1532.

188. *Loewen*, 129 F.Supp.3d at 952.

189. *Id*.

190. *Id*.

191. Cal. Civ. Code § 1670.5 commentary (2016).

192. Sonic-Calabasas A, Inc. v. Moreno, 57 Cal. 4th 1109, 1160 (Cal. 2013) (citation omitted).

193. Sanchez v. Valencia Holding Co., LLC, 61 Cal. 4th 899, 911 (Cal. 2015).

194. *Id*. (quoting Pinnacle Museum Tower Ass'n. v. Pinnacle Market Dev. (US), LLC, 55 Cal. 4th 223, 246 (Cal. 2012).

195. *Stirlen*, 51 Cal. App. 4th at 1536.

1. First Consideration: Facebook's Terms of Service and Data Policy Are Against California Public Policy and the Public Interest

Szetela v. Discover Bank provides the best illustration of a court deeming a contract term to be unconscionable due its contravention of established public policy. In the case, the court found a banking contract containing an adhesive arbitration provision to be substantively unconscionable because it "violate[d] public policy by granting Discover a 'get out of jail free' card while compromising important consumer rights."[196] The court reasoned that Discover had "essentially granted itself a license to push the boundaries of good business practices to their furthest limits, fully aware that relatively few, if any, customers will seek legal remedies, and that any remedies obtained will only pertain to that single customer without collateral estoppel effect."[197] In turn, the court found that the overwhelming advantages that the adhesive arbitration provision imparted on Discover contradicted "the California Legislature's stated policy of discouraging unfair and unlawful business practices."[198]

Facebook's non-consensual biometric data collection practices run afoul of Article I, Section I of the California Constitution, which prescribes an "inalienable right to privacy."[199] When California residents voted in 1972 to amend the state constitution to include an inalienable right to privacy, "the moving force behind the new constitutional provision was a more [focused] privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."[200]

The same pamphlet enticed voters to support the privacy amendment by noting that "[f]undamental to [consumer] privacy is the ability to control circulation of personal information . . . [t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives. Often we do not know that these records even exist and we are certainly unable to determine who has access to them."[201] These promises of privacy and the fears of simultaneous corporate and government overreaching are what charged California voters to amend their state constitution to explicitly include an inalienable right to privacy, a strong showing in favor of this highly important public policy.[202]

---

196. Szetela v. Discover Bank, 97 Cal. App. 4th 1094, 1101 (Cal. App. 4th 2002).
197. *Id*.
198. *Id*.
199. CAL. CONST. ART. I § 1.
200. White v. Davis, 13 Cal. 3d 757, 774 (Cal. 1975).
201. *Id*.
202. *Id*. (yet 42 years later, the driving factor behind the amendment remains true: "[a]t present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian").

If the privacy amendment was included to mitigate intrusive government data collection, as expressly recognized by the California Supreme Court,[203] then California courts need to take into account that over a mere six month period, Facebook complied with nearly 85% of domestic law enforcement requests for user data.[204] In fact, in a public-private surveillance quid pro quo of sorts, the government and Facebook have long worked together in pursuance of their respective agendas.[205] For example, where the U.S. Constitution may preclude the government from certain domestic surveillance measures, Facebook can supplement those deficiencies with datasets on its billion-plus users.[206] Similarly, where burdensome red-tape and regulations could limit the social media company's seemingly indomitable growth, the government can act to pave the way and knock down roadblocks standing in Facebook's way.[207]

This "you scratch my back, I'll scratch yours" partnership is facilitated by Facebook's Data Policy, which carves out a subjective standard for sharing user data with the government and law enforcement agencies.[208] By its very terms, Facebook's loose standard for deciding whether to access and share user data in response to a warrant, subpoena or other legal request is grounded in whether the company has "a good faith belief that the law requires [it] to do so."[209] Despite the fact that Facebook requires the government and law enforcement agencies to obtain a valid subpoena, search warrant, court order, or national security letter when seeking user data,[210] inclusion of the "good faith belief" catch-all significantly dismantles any purported legal privacy protections for Facebook users. "Good faith" is hardly a legal standard to which consumers or courts can look for sufficient clarity and guidance, and it does not adequately protect consumers' inalienable right to privacy as guaranteed by the California Constitution. Given the background behind

---

203. *See White*, 13 Cal. 3d at 761.

204. *See* FACEBOOK, Gov't Request Rep., https://govtrequests.facebook.com/country/United%20States/2016-H2/ (accessed July 27, 2017).

205. *Cf.* Bruce Schneier, *Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong*, THE ATLANTIC (Mar. 25, 2014), https://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/ and Cory Bennett, *Facebook accused of 'secretly lobbying' for cyber bill*, THE HILL (Oct. 26, 2015), http://thehill.com/policy/cybersecurity/258060-advocate-accuses-facebook-of-secretly-lobbying-for-cyber-bill (conflicting reports on whether Facebook lobbied Congress in support of the Cybersecurity Information Sharing Act (CISA), legislation which would have incentivized private companies to share data with the U.S. government on potential hacking threats).

206. *See* Bruce Schneier, The Public/Private Surveillance Partnership, Schneier on Security (Aug. 5, 2013), https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html.

207. *Id*. ("Corporations rely on the government to ensure that they have unfettered use of the data they collect.").

208. *Data Policy*, *supra* note 122.

209. *Id*.

210. *See* FACEBOOK, Law Enforcement Guidelines, https://www.facebook.com/safety/groups/law/guidelines/ (accessed July 10, 2017).

Article I, Section I, California courts need to recognize that Facebook's Terms of Service and Data Policy deliberately and utterly take away the rights of consumers to control the collection and dissemination of their biometric data.

2. Second Consideration: Facebook's Terms of Service and Data Policy Impose an Unreasonable and Unexpected Allocation of Risk

The overly harsh allocation of risk in Facebook's policies falls squarely on the back of consumers. Facebook reaps the overwhelming advantages of its collection of users biometric identifiers despite the company's Data Policy and Terms of Service being "unreasonably favorable to the more powerful party."[211] For example, Facebook's Data Policy states that the company can share user information within its 11 other Facebook-owned companies,[212] as well as any applications, websites and any third-party integrations on or using Facebook.[213] Facebook further states that "[i]f the ownership or control of all or part of our Services or their assets changes, [the company] may transfer your information to the new owner."[214] Even if a user simply deletes a photograph from his or her account, Facebook's Terms of Service states that any "removed content may persist in backup copies for a reasonable period of time (but will not be available to others)."[215] However, this provision conveniently seems to reason that users are only worried about other users having access to their removed content, rather than Facebook retaining the licensed right to use, distribute or sell any deleted user data to any entity or individual that Facebook so chooses.[216] But this conclusion is in contradiction with the summary findings below in Figure B, which demonstrate that, as a whole, consumers are more worried about how companies are collecting, distributing, and sharing their personal data.[217]

In fact, this 2015 study showed that the top two consumer privacy concerns are where and to whom data is sold and where data is kept.[218] Yet, despite such pervasive consumer privacy concerns, Facebook's Terms of Service and Data Policy artfully includes ambiguous phrases like "as long as" and "for a reasonable period" that essentially grant to the company

211. *See Loewen*, 129 F.Supp.3d at 952 (citing 8 Williston on Contracts (4th ed.2010) § 18.10, p. 91).

212. For a full list of Facebook's 11 owned companies, *see* FACEBOOK, https://www.facebook.com/help/111814505650678 (accessed Apr. 2, 2017).

213. *Data Policy*, *supra* note 122.

214. *Id*.

215. *Terms of Service*, *supra* note 106.

216. *See* Chirita, *supra* note 147, at 3 (noting that "personal data, which is economically relevant, could be misused, for instance, through it being shared with third parties, in order to maintain or strengthen a dominant market position").

217. *See* Stacey Higginbotham, *Companies need to share how they use our data. Here are some ideas*, FORTUNE MAGAZINE (July 6, 2015), http://fortune.com/2015/07/06/consumer-data-privacy/ (citing Jessica Groopman, *Consumer Perceptions of Privacy in the Internet of Things*, ALTIMETER GROUP (2015), http://go.pardot.com/l/69102/2015-07-12/pxzlm).

218. *Id.*

indisputable and unbounded access to all user data, leaving users in the dark as to who has their information and who might get it next.[219] All things considered, a court would not be hard-pressed in finding that Facebook's Terms of Service and Data Policy contain unreasonably favorable terms for the company.

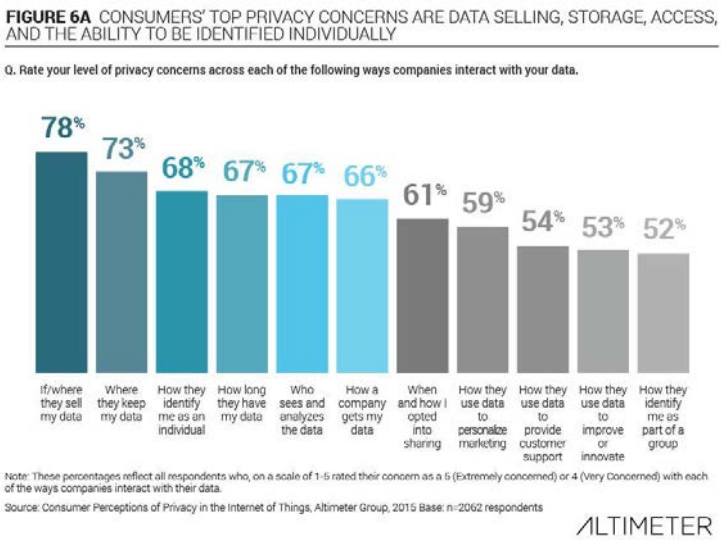

Figure B [220]

With no concrete justification, and operating only under conditions of self-restraint, Facebook's Terms of Service and Data Policy allow the company to continue to sweep in a massive amount of sensitive user data, seemingly just to have it.

Further, there is certainly an unexpected allocation of risk in the Terms of Service and Data Policy, as they seem to be written in a way that is advantageous solely to Facebook. What is troubling, then, is that

219. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 122; *see also* Lynch, *supra* note 10, at 11 ("[a]ll of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large").

220. Higginbotham, *supra* note 217 (citing Jessica Groopman, *Consumer Perceptions of Privacy in the Internet of Things*, ALTIMETER GROUP (2015), http://go.pardot.com/l/69102/2015-07-12/pxzlm).

government,[221] law enforcement agencies,[222] app developers,[223] and advertisers[224] all have an interest in user information collected by Facebook. Similar to *Szetela*, Facebook's Terms of Service and Data Policy essentially grant the company a license to push the boundaries of sound business practices, as the company is retaining an alluring goldmine of data that can be shared or sold without user consent.[225] Considering that Facebook operates according to its own subjective standards of "good faith" and has historically failed to "maintain control over how user data is used by advertisers,"[226] the outside interest in the sheer amount of personal user data retained by Facebook and the company's reserved right to use it at its discretion lends support to a conclusion that the terms are unreasonably unfair and function only to the detriment of consumers.

For example, Facebook could potentially share or sell[227] its entire data set to the federal government, subjecting millions of users to unwarranted surveillance and inclusion in the FBI facial recognition database.[228] Facebook's dataset is attractive because even the FBI, through its Next Generation Identification ("NGI") facial recognition database, pales in

221. *See generally* John Lynch & Jenny Ellickson, U.S. Dep't of Justice, *Computer Crime and Intellectual Property Section, Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, Linkedln, and More*, (Mar. 2010), 17, http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf.

222. *See generally* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 129, at 19; *see also* Julie Masis, Is this Lawman your Facebook Friend?, BOSTON GLOBE, Jan. 11, 2009, http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend?mode=PF.

223. *See generally* ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 129, at 17–18.

224. *Id*.

225. *See* Weinstein, *supra* note 15 ("By clicking the 'I Agree' button, you blindly assent to hand over your life and interests to billion-dollar corporations to do with it what they may. Oftentimes, this means selling your information to the highest bidder or sharing it with your government. Most of us never even realize it. Our government does, Republicans and Democrats alike, but does nothing about it. After all, this data is a treasure trove they can access by simply reaching into the data candy bowl collected by Facebook, Google, and company.").

226. ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 129, at 18.

227. *See, e.g.*, Lauren Effron, *Facebook In Your Face: New Facial Recognition Feature Raises a Few Eyebrows*, ABC NEWS (June 10, 2011), http://abcnews.go.com/Technology/facebook-facial-recognition-feature-raises-eyebrows/story?id=13792666 (quoting Graham Cluely, a senior technology consultant at British Internet security firm Sophos: "Maybe in the future [Facebook] will sell this information to third parties . . . [t]here's so much information we've already given away willingly to Facebook. They have slowly eroded away our control over that data.").

228. Facebook further reserves the right to share user information in response to legal or governmental requests so long as the company has a "good faith belief" that the law requires their acquiescence. *See* Facebook https://www.facebook.com/about/privacy/ (accessed Apr. 5, 2017). Biometric identifiers collected through facial recognition are included in such requests, as the U.S. Department of Justice has indicated that the "standard data production" from Facebook contains "photoprint" and individual contact information, as well as "other data" available upon request, noting that Facebook is "often cooperative with emergency requests." Lynch & Ellickson, *supra* note 221, at 17.

comparison to Facebook's accuracy with facial recognition.[229] The difference in accuracy likely can be attributed to the fact that the FBI is often working with one frontal-facing photograph, usually in the form of a mug shot, passport photo, or driver's license photo,[230] while Facebook's algorithm is consistently being refined and improved each time a user uploads a photo and tags someone.[231] This is because each tag "shows the algorithm what someone looks like from different angles and in [a] different light[]."[232] So while other facial recognition systems struggle with adapting to aging subjects, inconsistent lighting, and single, front-facing photos,[233] Facebook's database and algorithm is uniquely precise because it is routinely updated and cultivated[234] by the company's 1.65 billion users.[235]

Yet, the glaring issue remains: Facebook's diligently developed facial recognition database is arguably lacking user consent, as there is no explicit mention of facial recognition technology included in the company's Terms of Service or Data Policy to which users could even contemplate consenting.[236] Consequently, users who click "I Agree" in a brief pop-up are agreeing to quite possibly be subject to inclusion in government surveillance or to have their sensitive biometric information shared and distributed with any other entity – at no risk or cost to Facebook whatsoever and without any prior notice to consumers.[237]

---

229. Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, ELECTRONIC FRONTIER FOUNDATION (Apr. 14, 2014), https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year (to illustrate, when given a particular face, NGI provides a list of 50 potential facial matches – but of those 50 possibilities, the FBI reports an unimpressive 85% accuracy in successful facial recognition).

230. *See* Jennifer Lynch, *New Report: FBI Can Access Hundreds of Millions of Face Recognition Photos*, ELECTRONIC FRONTIER FOUNDATION (June 15, 2016) https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos; *see also* Naomi Lachance, *Facebook's Facial Recognition Software Is Different From The FBI's. Here's Why*, NATIONAL PUBLIC RADIO (May 18, 2016), (http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why.

231. *See* Naomi Lachance, *Facebook's Facial Recognition Software Is Different From The FBI's. Here's Why*, NATIONAL PUBLIC RADIO (May 18, 2016), http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why ("Every time you tag a photo, you're adding to an enormous, user-driven wealth of knowledge and data.").

232. *Id*.

233. Yue Liu, *supra* note 41, at 41.

234. *See, e.g.*, Martin Kaste, *A Look Into Facebook's Potential To Recognize Anybody's Face*, National Public Radio (Oct. 28, 2013), http://www.npr.org/sections/alltechconsidered/2013/10/28/228181778/a-look-into-facebooks-potential-to-recognize-anybodys-face ("Theoretically, every time you label faces by tagging a picture, you're chipping away at those two big challenges for universal facial recognition. First, you're helping to build a super-database of labeled faces. Second, you're uploading multiple versions of each person's face, which can improve a system's accuracy.").

235. Lachance, *supra* note 231.

236. *See Terms of Service*, *supra* note 106; *Data Policy*, *supra* note 116.

237. *See, e.g.*, Weinstein, *supra* note 15.

Several California courts have agreed that substantive unconscionability "turns not only on a 'one sided' result, but also on an absence of 'justification' for it."[238] The California Supreme Court has recognized that "lack of mutuality can be manifested as much by what the agreement does not provide as by what it does."[239] Outlined in *Armendariz v. Foundation Health Psychcare Services, Inc*., the California Supreme Court was receptive to the fact that even where a provision is not "expressly authorize[d]" in a contract, the Court can look to the "clear implication of the agreement" to establish a lack of mutuality.[240] Even in cases where there is a "reasonable justification for [a] lack of mutuality,"[241] California courts have found substantive unconscionability in contractual provisions where certain terms are fashioned unfairly and solely for "means of maximizing employer advantage."[242]

a. *Lack of Justification for the One-Sided Terms*

Because Facebook does not expressly mention facial recognition technology and its biometric data collection practices in its Terms of Service and Data Policy, a California court should then look to the "clear implication of the agreement"[243] to establish a lack of mutuality. It is unlikely that there would be any possible justification for the lack of mutuality in Facebook's failure to explicitly mention its use of facial recognition technology in the two agreements to which users are required to consent. The only time Facebook provided a justification regarding its implementation of facial recognition technology was during a congressional hearing, in which the company stated that it wanted to make photos "more social."[244] But users could manually tag photos, keeping the "social" aspect alive, prior to Facebook's introduction of facial recognition technology.[245] Facebook contends that "many people" told the company that "manually entering tags for each person in every photo required a great deal of time and effort."[246] But this was a bare assertion, as Facebook offered no surveys or inquiries demonstrating that a substantial

238. *Carboni*, 2 Cal. App. 4th at 84; *see also A & M Produce Co.*, 135 Cal. App. 3d at 487.

239. *Armendariz*, 24 Cal. 4th at 120.

240. *Id*.

241. Soltani v. W. & S. Life Ins. Co., 258 F.3d 1038, 1046 (9th Cir. 2001).

242. *Id*.

243. *Armendariz*, 24 Cal. 4th at 120.

244. *See What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) (testimony of Richard Sherman, Manager of Privacy & Public Policy at Facebook), https://www.judiciary.senate.gov/imo/media/doc/12-7-18ShermanTestimony.pdf.

245. *Id*. at 4.

246. *Id*.

number of users were deeply opposed to manual tagging to warrant the implementation of facial recognition technology as the sole alternative.[247]

3. Third Consideration: The Lack of Mutuality in Facebook's Terms of Service and Data Policy Is Not Due to a Legitimate Commercial Need

One might argue that Facebook is not the only business operation imposing such broad and wide-reaching terms onto consumers, suggesting that the proper test for unconscionability might be whether the contract provisions are "so extreme as to appear unconscionable according to the mores and business practices of the time and place."[248] Although the current business practice for companies may be to write overreaching privacy policies for consumers by way of standardized agreements, that does not mean the business practice is ethically sound, nor that such privacy policies are necessarily immune from a finding of unconscionability.[249]

Moreover, Facebook is not acting like all other businesses with respect to how it operates its facial recognition data collection. Google also has a facial recognition feature, but unlike Facebook, Google intentionally leaves the recognition feature off by default and allows users to elect whether or not to opt-in.[250] Facebook could have set up its facial recognition system so that users would have to affirmatively opt-in, rather than opt-out of the feature, something which was suggested to the company in 2012.[251] But Facebook deliberately maintained the facial recognition collection as an opt-out program, meaning that biometric identifiers are collected by default unless

---

247. *Id*. at 5 (noting that "[t]ag suggestions has been enthusiastically embraced by millions of people" but offering no qualitative data on the public reception of tag suggestions). In fact, several articles were published after the initial rollout indicating that the suggestions were not enthusiastically embraced at all. *See, e.g.*, Lauren Effron, *Facebook In Your Face: New Facial Recognition Feature Raises a Few Eyebrows*, ABC NEWS (June 10, 2011), http://abcnews.go.com/Technology/facebook-facial-recognition-feature-raises-eyebrows/story?id=13792666 (quoting Graham Cluely, a senior technology consultant at British Internet security firm Sophos: "There's a huge backlash in response.... [Facebook users] don't really like the idea of Internet companies, Facebook in particular, gathering data of what we look like . . . it makes me uncomfortable...especially when they turn on features like this without even telling us"); *see also* Nathan Olivarez-Giles, *Facebook under scrutiny for face-recognition feature from privacy group, lawmakers*, L.A. TIMES (June 8, 2011), http://articles.latimes.com/2011/jun/08/business/la-fi-0609-facebook-faces-mobile.

248. 1 Corbin, *Contracts* (1963) § 128, 551.

249. *See* TERMS OF SERVICE; DIDN'T READ, https://tosdr.org/ [https://perma.cc/44TB-H6VC] (accessed Apr. 5, 2017) (rating various networking platforms and websites for consumers based on the broad, wide-reaching nature of company privacy policies, copyright licenses, and more).

250. *Facial Recognition Hearing*, *supra* note 49, at 26 (statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

251. *Id*. at 26. *See also* FTC, BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES iii (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf [https://perma.cc/Q8FT-PTCZ].

and until the particular user manually changes his or her privacy settings.[252] Despite years of criticism and conversation, Facebook continues to collect its users biometric identifiers by default, meaning the company is unequivocally collecting this sensitive personal data absent explicit consent from well over a billion people.[253]

This note does not purport to say that Facebook should refrain from issuing standardized form agreements to its users, nor does it purport to say that Facebook should allow each user to negotiate the terms with the company. It would be preposterous to have Facebook negotiate its user agreements with each and every one of its billion-plus users. Standardized agreements undoubtedly offer "a degree of efficiency, simplicity, and stability," and they "appear to be a necessary concomitant of a sophisticated, mass-consumption economy."[254] However, "the obvious danger exists that the party who draws up the contract will do so unfairly to his or her advantage,"[255] which is what Facebook is currently doing to its users through the company's Terms of Service and Data Policy. As noted in *Stirlen*, there is no "legitimate commercial need" for Facebook to accrue its user's biometric data and subsequently take away any ownership right over that data from its users.

IV. SOLUTION: WITH MULTIPLE LEGAL CHANNELS AVAILABLE, CALIFORNIA COURTS ARE BEST POSITIONED TO STRIKE DOWN FACEBOOK'S PRIVACY-INVASIVE TERMS REGARDING THE COMPANY'S USE OF FACIAL RECOGNITION TECHNOLOGY

Pursuant to Section 15 of Facebook's Terms of Service, any claims related to Facebook are to be governed by California law and resolved "exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County."[256] Aside from being the mandated jurisdiction due to Facebook's forum and conflict of laws provision, the California judiciary is actually best positioned to take the lead in protecting consumer privacy rights from Facebook's overarching biometric data collection practices. The standing requirement to bring a claim in a California state court, such as San Mateo County, is very straightforward:

252. *See* Adams-Heard, *supra* note 181 ("The technology powers a photo feature called 'tag suggestions' that is automatically turned on when users sign up for a Facebook account . . . Users can opt-out at any time, Facebook said. But that requires that they [affirmatively act to] change their settings.").

253. *See* Graham Cluely, *Facebook changes privacy settings for millions of users – facial recognition is enabled*, SOPHOS (June 7, 2011), https://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/ [https://perma.cc/E6XQ-EADH].

254. *Sybert*, *supra* note 94, at 297–98.

255. *Id*.

256. *Terms of Service*, *supra* note 106.

Article VI, §10 of the state constitution grants Superior Courts power to hear relatively any cause of action.[257] The only threshold requirement is dictated by the California Code of Civil Procedure, which mandates that "every action must be prosecuted in the name of the real party in interest."[258] The U.S. District Court for the Northern District of California, on the other hand, is a federal court, meaning that a plaintiff would need to meet the standing requirements as imposed by Article III of the U.S. Constitution.[259] Regardless of the forum, California courts have the following three legal avenues available to strike down Facebook's privacy-invasive terms: state contract law, state constitutional law, and state tort law. Each possibility is discussed respectively below.

A. Option No. 1: Unconscionability

Based on the extensive reasoning in Section III above, California courts should find that Facebook's Terms of Service and Data Policy containing unconscionable terms with respect to the company's secretive and non-consensual biometric data collection practices under state law. Pursuant to the California Civil Code, "[i]f the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result."[260] The Code offers courts a great deal of flexibility in striking the proper balance between consumer privacy and Facebook's desire to further its utilization of new technologies. For example, rather than dismantling Facebook's Terms of Service and Data Policy in its entirety, California courts could begin by voiding the provisions providing or inferring unrestricted access to user's biometric data.[261]

In order for a California court to deem provisions within Facebook's Terms of Service and Data Policy unconscionable, a Facebook user would need to bring suit alleging that he or she was injured by Facebook's use of

257. CAL. CONST. Art. VI, §10.

258. Cal. Code Civ. Proc. §367 (2017).

259. "To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

260. Cal Civ Code § 1670.5 (2016).

261. *See* Future of Privacy Forum, Privacy Principles for Facial Recognition Technology, Discussion Document (Dec. 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf. (recommending that "companies should also set reasonable retention and disposal practices for facial recognition data. Facial recognition template data that can be used to personally identify an individual, as opposed to aggregate information or simple detection or classification data, should be retained no longer than necessary for legitimate business purposes, and deleted or destroyed in a secure manner").

facial recognition technology and collection of biometric data.[262] Likely, the critical issue that the litigation would turn on would be the question of whether the Facebook user suffered an injury. This determination would be based on whether the user was "sufficiently informed about how their Facebook data would be used"[263] and whether the user "gave permission or agreed to give consent to the company[] to collect, store and tag a photo of their face."[264]

One could argue that if or until Facebook actually does sell its facial recognition database, or until a significant biometric breach occurs, users have not suffered concrete harm or particularized injury under Article III[265] of the U.S. Constitution from the company's collection of biometric identifiers. However, in *Spokeo, Inc. v. Robins*, the U.S. Supreme Court acknowledged that the "risk of real harm" may satisfy the Article III concrete injury requirement where "harms may be difficult to prove or measure."[266] The *Spokeo* Court further acknowledged that "'[c]oncrete' is not . . . necessarily synonymous with 'tangible.'"[267]

Taking Article III and *Spokeo* into consideration, there are two apparent risks of real harm to Facebook users with regard to the company's utilization of facial recognition technology. First, operating with no restraint and with little regard for consumers, Facebook is already engaged in profiting off of user data and information.[268] Estimated to be responsible for roughly 38%[269] of all advertisement revenue growth in the United States, Facebook's wealth

262. *See* California Courts, *Filing a Lawsuit*, http://www.courts.ca.gov/9616.htm (accessed Apr. 5, 2017). This section presupposes that a consumer would bring suit in the Northern District of California, a federal court, solely based on the fact that the most recent and preeminent litigation involving Facebook and its users was brought in this court. *See* In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD at 1 (N.D. Cal. 2016) (discussed *infra*).

263. *See* Meg Graham, *What's Next Illinois Biometrics Lawsuits May Help Define Rules for Facebook, Google*, CHI. TRIB. (Nov. 26, 2017, 2:57 P.M.), http://www.chicagotribune.com/bluesky/originals/ct-biometric-illinois-privacy-whats-next-bsi-20170113-story.html.

264. *See* Kate MacArthur, *Facebook, Google track you, but how is data being shared?*, CHI. TRIB. (Apr. 20, 2016, 5:26 A.M.), http://www.chicagotribune.com/bluesky/originals/ct-carla-michelotti-biometric-tracking-bsi-20160420-story.html.

265. "To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

266. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) (citing *Clapper*, 133 S. Ct. 1138 (2013)).

267. *Spokeo*, 136 S. Ct. at 1549.

268. *See* MacLean, *supra* note 12, at 45 ("In the digital age, when private consumer data—through the wideopen 'back door'—is so freely captured, used, resold, reused, aggregated, and more, for profit alone and largely without the knowing and voluntary consent of the consumer subject of the data, our right to privacy has been eroded almost beyond repair").

269. *See* Jason Kint, *Google and Facebook devour the ad and data pie. Scraps for everyone else*, DIGITAL CONTENT NEXT (June 16, 2016), https://digitalcontentnext.org/blog/2016/06/16/google-and-facebook-devour-the-ad-and-data-pie-scraps-for-everyone-else/.

of data that it has amassed on its billion-plus users results in an 89% accuracy rate for targeted advertisements.[270]

In 2015 alone, Facebook garnered a $4 billion profit from advertising revenues.[271] Due to the sheer magnitude of user data and its accuracy in targeted advertising services, Facebook is poised to remain an attractive choice for advertising sales. Yet the problem remains that due to the broad nature of its Terms of Service and Data Policy, Facebook fundamentally has no limitations on the extent to which it can go in selling[272] user data and information.[273] This problem is further enhanced by the fact that there is no accountability framework for Facebook, and consumers have relatively no possible way to trace their biometric data through any subsequent sale or distribution.

In Re Facebook Biometric Information Privacy Litigation, which is currently pending in the Northern District of California, signals a possible shift in the willingness of California courts to find that Facebook's collection and retention of face prints from uninformed consumers could suffice as a concrete injury for consumers.[274] Facebook filed a motion to dismiss the lawsuit arguing that under *Spokeo*, the plaintiffs failed to allege a concrete injury resulting from the company's facial recognition tagging practices.[275] Facebook's argument was "that the collection of biometric information without notice or consent can never support Article III standing without 'real-world harms' such as adverse employment impacts or even just 'anxiety.'"[276]

---

270. *See* FACEBOOK, *Reach new customers with your targeting*, https://www.facebook.com/business/a/online-sales/targeting-tips-basic (visited Feb. 8, 2017).

271. Kint, *supra* note 269.

272. *See, e.g.*, Jared Bennett, Center for Public Integrity, *Facebook: Your Face Belongs to Us*, The Daily Beast (July 31, 2017), https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition [https://perma.cc/DHJ4-AHRG] (quoting Larry Ponemon, founder of the Ponemon Institute: "The whole Facebook model is a commercial model . . . gathering information about people and then basically selling them products" based on that information).

273. Facebook is prone to acting first and dealing with the consequences later. For example, in 2013 Facebook settled a class-action lawsuit for roughly $20 million for sharing data with advertising companies on its users' "likes" without consent. Similarly, in 2016 the company came under fire for selling targeted advertisements based on race and ethnicity. *See* Sapna Maheshwari and Mike Isaac, *Facebook Will Stop Some Ads From Targeting Users by Race*, N.Y. TIMES (Nov. 11, 2016), https://www.nytimes.com/2016/11/12/business/media/facebook-will-stop-some-ads-from-targeting-users-by-race.html?_r=0.

274. *See* In Re Facebook Biometric Information Privacy Litigation, Case No. 15-cv-03747-JD (N.D. Cal. 2016) (the plaintiffs are suing Facebook for the company's facial recognition tagging practices under the Illinois' Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b) (2008), http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 [https://perma.cc/NH9E-J5R3].

275. *See generally* In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD (N.D. Cal. Sept. 14, 2016) (Facebook, Inc.'s Motion to Dismiss for Lack of Subject-Matter Jurisdiction).

276. In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD, at 7 (N.D. Cal. Feb. 26, 2018) (Order Denying Facebook's Renewed Motion to Dismiss for Lack of Subject Matter Jurisdiction).

In a November 2017 hearing on the matter, U.S. District Judge James Donato seemed unconvinced by Facebook's *Spokeo* argument, stating that "[t]he right to say no is a valuable commodity," also adding that the litigation involves "the most personal aspects of your life: your face, your fingers, who you are to the world."[277] Judge Donato subsequently issued an order denying Facebook's motion to dismiss in February 2018. Quoting the *Spokeo* Supreme Court, Judge Donato delineated the elements required to establish standing, stating that "a plaintiff must demonstrate standing to sue by alleging the 'irreducible constitutional minimum' of (1) an 'injury in fact' (2) that is 'fairly traceable to the challenged conduct of the defendants' and (3) 'likely to be redressed by a favorable judicial decision.'"[278] Importantly, Judge Donato reiterated that "[t]he specific element of injury in fact is satisfied when the plaintiff has 'suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."'"[279] Judge Donato further explained that although "*Spokeo* []refers to Congress, [] state legislatures are equally well-positioned to determine when an intangible harm is a concrete injury."[280]

Of course, *In Re Facebook Biometric Information Privacy Litigation* is unique in the sense that involves a very particularized Illinois state statute. This case is predicated upon Illinois' Biometric Information Privacy Act, which "codifie[s] a right of privacy in personal biometric information" in order to give "Illinois residents the right to control their biometric information by requiring notice before collection and giving residents the power to say no by withholding consent."[281] As a result, "[w]hen an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air."[282] As Judge Donato concluded, "[] the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt."[283]

Although California does not have a biometric privacy law on point that resembles Illinois', the California Civil Code provides California residents with other statutorily created interests that can and should be protected against Facebook's intrusive facial recognition technology practices. Judge Donato explicitly mentioned that the Ninth Circuit had previously established that

277. Joel Rosenblatt, *Facebook Judge Frowns on Bid to Toss Biometric Face Print Suit*, Bloomberg (Nov. 30, 2017), https://www.bloomberg.com/news/articles/2017-11-30/facebook-judge-frowns-on-bid-to-toss-biometric-face-print-suit [https://perma.cc/M3GH-HANY] (concluding "[t]he point is Illinois gave its citizens the right to say no . . . [t]he allegation is Facebook usurped that right. That is not a mere technicality in my view.").

278. *See* Case No. 15-cv-03747-JD, at 3 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016)).

279. *Id.* at 3–4 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

280. *Id.*at 4.

281. *Id.* at 6.

282. *Id.*

283. *Id.*

"'state law can create interests that support standing in federal courts. If that were not so, there would not be Article III standing in most diversity cases, including run-of-the-mill contract and property disputes. State statutes constitute state law that can create such interests.'"[284] That being said, California courts can use the state's civil code[285] to plausibly render Facebook's Terms of Service and Data Policy unconscionable for automatically opting users into its facial recognition technology programs after failing to explicitly state that the company collects its users' biometric data upon sign-up.

Consumers could face an uphill battle in California, however, as state judges have remarked that "even though injury-in-fact may not generally be Mount Everest . . . in data privacy cases in the Northern District of California, the doctrine might still reasonably be described as Kilimanjaro."[286] However true that might be, Judge Donato's recent ruling is promising for consumer privacy efforts with respect to facial recognition technology.

The second risk of harm stems from the fact that Facebook disclaims relatively all liability for any ensuing privacy and security implications that might follow in the event of a biometric data breach. This risk is derived from the company's significantly broad inclusion of an exculpatory clause, essentially carving out any liability for Facebook in the event that anything happens to user biometric data that is later sold or accessed by third parties.[287]

This free-trade, zero-liability exception that Facebook has reserved for itself raises an unprecedented risk to consumers, as "it could be difficult or impossible for [consumers] to determine what data has been collected about them, how it is being used, who it has been shared with, and to request access to correct errors or delete the information."[288] Due to "the fact that face images can be captured without [detection] and in public,"[289] the risk of real harm to consumers is undeniable. The reality is that "[a]ll of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large."[290]

Accordingly, another way California courts could limit the offending terms is by explicitly excluding facial recognition data from the scope of Facebook's exculpatory clause. For decades now, several California courts have invalidated contracts containing exculpatory clauses that "affect[] the

284. *Id*. at 4 (quoting Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001)).

285. Cal Civ Code § 1670.5 (2016).

286. In re Google, Inc. Privacy Policy Litig., 2013 U.S. Dist. LEXIS 171124, at *13 (N.D. Cal. Dec. 3, 2013).

287. *See* Facebook Terms of Service, https://www.facebook.com/terms.php (accessed July 31, 2017).

288. Future of Privacy Forum, Privacy Principles for Facial Recognition Technology, Discussion Document (Dec. 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

289. Lynch, *supra* note 10, at 16.

290. *Id*.

public interest."[291] Included in its Terms of Service, the exculpatory clause releases Facebook from any liability resulting from abusive data practices or bad-faith actions from third parties, such as advertisers.[292] This is troubling because "Facebook is one of the most well-known businesses that mine our personal information and sell it to third party companies who use the information in their behavioral advertising strategies."[293] Because the consequences of a biometric data breach can have massive and potentially permanent security consequences, California courts would be well served to invalidate the applicability of Facebook's exculpatory clause to facial recognition data.[294]

Adhesion contracts, like Facebook's, do not have to be completely eradicated in order to better protect consumers; rather, California courts simply need to be more proactive in shielding consumers from overbearing adhesion contracts containing overzealous and unconscionable terms, especially when something as significant as biometric data is on the line. If presented with the opportunity, California courts should decline to enforce Facebook's current Terms of Service and Data Policy on the grounds of unconscionability. Facebook should then be required to revise its Terms of Service and Data Policy so that prospective users are provided with full and explicit notice of the company's biometric data collection practices, including a retention and destruction schedule for such data, before creating an account. Additionally, California courts should require Facebook to operate its tag suggestions exclusively as an opt-in program so that the company has no opportunity to automatically accumulate and hold onto sensitive biometric data. If ever presented with the opportunity to do so, there are a number of sound ways for California courts to limit the unconscionable provisions included in Facebook's Terms of Service and Data Policy without invalidating the entirety of these user agreements.

---

291. *See* Tunkl v. Regents of Univ. of Cal., 60 Cal. 2d 92, 98 (Cal. 1963) (stated best by the California Supreme Court, "[n]o definition of the concept of public interest can be contained within the four corners of a formula. The concept, always the subject of great debate, has ranged over the whole course of the common law"); *see also* Hiroshima v. Bank of Italy, 78 Cal. App. 362 (1926); Union Constr. Co. v. Western Union Tel. Co., 163 Cal. 298 (Cal. 1912)).

292. *See* Facebook Terms of Service, https://www.facebook.com/terms.php (accessed July 31, 2017) (the exculpatory clause reads: "WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE OR THAT FACEBOOK WILL ALWAYS FUNCTION WITHOUT DISRUPTIONS, DELAYS OR IMPERFECTIONS. FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES").

293. Justin McHugh, *I Know Who You Are and I Saw What You Did [Social Networks and The Death of Privacy*, 31 SYRACUSE SCI. & TECH. L. REP. 132, 137 (2015) (citing Lori Andrews, I Know Who You Are and I Saw What You Did (Free Press ed., 2011) at 19.

294. *See, e.g.*, Future of Privacy Forum, *supra* note 261 ("social networks and other large databases of identified individual images could increasingly become the targets of access by unauthorized individuals, leading to consumers' facial recognition data being used in ways that consumers cannot anticipate or control, and without their knowledge.").

B. Option No. 2: California State Constitution and Public Policy

If California courts are dissuaded from finding that Facebook's Terms of Service and Data Policy to constitute an unconscionable contract, state courts should still find Facebook's terms independently unlawful, as they clearly violate well-established California public policy as indicated in the state constitution. The First Amendment of the California State Constitution explicitly prescribes a right to privacy, stating:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[295]

Although the right to privacy is not absolute,[296] several California courts have found the state constitution's explicit inclusion of an inalienable right to privacy to be a sufficiently stated interest.[297] Under California law, contacts are void as contrary to public policy where they violate or implicate larger social constructs and concerns.[298] The concept of invalidating contracts on public policy grounds is far from novel to the California judiciary. For example, as far back as 1928, California's 1st District Court of Appeal stated: "public policy means the public good. Anything which tends to undermine that sense of security for individual rights, whether of personal liberty or private property, which any citizen ought to feel is against public policy."[299]

An argument that consumers waive their right to privacy when accepting Facebook's Terms of Service and Data Policy is thwarted by Cal. Civil Code § 3513, which states: "any one may waive the advantage of a law intended solely for his benefit. But a law established for a public reason cannot be contravened by a private agreement."[300] In determining whether a law was intended for personal or public benefit, California courts have historically found that a "law has been established 'for a public reason' only if it has been enacted for the protection of the public generally, i.e., if its tendency is to promote the welfare of the general public rather than a small percentage of citizens."[301]

It is plain from looking at the legislative history behind Article 1 Section 1 of the California Constitution that the inalienable right to privacy was included for the public benefit. The bill's sponsor "was concerned about

---

295. CAL. CONST. ART. I § 1 (emphasis added).

296. *See* CAL. CONST. ART. I § 1.

297. *See, e.g.*, In re Carrier IQ, Inc., Consumer Privacy Litig., 78 F. Supp. 3d 1051, 1117 (N.D. Cal. 2015); *White*, 13 Cal. 3d at 773–74 (Cal. 1975).

298. *See* 2-18 MB Practice Guide: CA Contract Litigation 18.10.

299. Noble v. Palo Alto, 89 Cal. App. 47, 51 (Cal. App. 1928).

300. Cal. Civ. Code § 3513 (2016).

301. *See* Benane v. Int'l Harvester Co., 142 Cal. App. 2d Supp. 874, 878 (Cal. App. 1956); *accord* In re Application of Kazas, 22 Cal. App. 2d 161, 172 (Cap. App. 1937); Cal. Bank v. Stimson, 89 Cal. App. 2d 552, 554 (Cal. App. 1949); Winklemen v. Sides, 31 Cal. App. 2d 387 (Cal. App. 1939).

the evils associated with the growing tendency of the government to collect large amounts of private information about people . . . perceiv[ing] [the] government's collection and use of such information as part and parcel of a shrinking orbit of privacy."[302] Perhaps more telling, the legislative history reveals that the bill was introduced due to concern around "government cooperation with private business in the widespread dissemination of private information" as well as concern about "private businesses knowing private facts about private people."[303] As the legislative history illustrates, privacy rights were incorporated into the state constitution for the public welfare. Therefore, California courts should find that Article 1 Section 1 cannot be circumvented by a private agreement between Facebook and its users. Moreover, the fact that the California judiciary holds that "courts should indulge every reasonable presumption against a waiver of a constitutional right"[304] lends support to a pro-consumer, pro-privacy finding with respect to Facebook's Terms of Service and Data Policy.

Even supposing that a court were to assume that Facebook users waived their state constitutional right to privacy, it is well-established in California case law that "[w]aiver always rests upon intent. Waiver is the intentional relinquishment of a known right after knowledge of the facts."[305] Facebook users simply cannot have relinquished their inalienable right to privacy because, in doing so, they would have needed to know the full extent of how Facebook was using their biometric data, what state privacy rights they had, and what relinquishment of those privacy rights actually entailed. California courts have previously accepted invasion of privacy as a valid public policy concern and there is no reason why the courts should shy away from protecting consumers from Facebook's most recent privacy-invasive practices with facial recognition.[306]

When the legislature sought to amend the state constitution in 1972, California residents received a state election pamphlet which stated that the inalienable right to privacy was included to "prevent[] government and business interests from collecting and stockpiling unnecessary information about [consumers] and from misusing information gathered for one purpose in order to serve other purposes or to embarrass [consumers]."[307] Analogous

---

302. *See* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 2, 418 (1992), http://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1631&context=plr.

303. *Id*.

304. *See* People v. Houston, 10 Cal. App. 3d 894, 900 (Cal. App. 1970).

305. *See* Kay v. Kay, 188 Cal. App. 2d 214, 218 (Cal. App. 1961) (quoting Wienke v. Smith, 179 Cal. 220, 226 (Cal. 1918)) (citing Alden v. Mayfield, 164 Cal. 6, 11 (Cal. 1912) (finding no valid waiver where one attempts "surreptitiously to do something which might in some way advantage him")); *see also* Freshko Produce Servs. v. Produce Delights, LLC, 2017 U.S. Dist. LEXIS 57004 at *4 (C.D. Cal. Apr. 13, 2017).

306. *See, e.g.*, In re Carrier IQ, Inc., Consumer Privacy Litig., 78 F. Supp. 3d 1051, 1117 (N.D. Cal. 2015); Pioneer Elec. (USA), Inc. v. Superior Court, 40 Cal. 4th 360, 370 (Cal. 2007) ("the right of privacy protects the individual's *reasonable* expectation of privacy against a *serious* invasion").

307. White v. Davis, 13 Cal. 3d 757, 774 (Cal. 1975).

to Judge Donato's reasoning used in *In Re Facebook Biometric Information Privacy Litigation*, the California legislature clearly intended to protect consumers against the kind of intrusive and sweeping data collection practiced by Facebook.[308] Since it is well-regarded that "'state law can create interests that support standing in federal courts,'"[309] California courts can use the California State Constitution's inalienable right to privacy in order to protect consumer privacy rights against Facebook's intrusive biometric data collection practices.

By ignoring the will of the people who voted to include an inalienable right to privacy in the now long-standing Constitutional principle, California courts will be engaging in an unprecedented level of judicial activism, with the burden falling squarely on the backs of consumers.

C. State Tort Law: Intrusion Upon Seclusion

Lastly, this issue could potentially be addressed from a tortious conduct standpoint by focusing on the state tort of intrusion upon seclusion. California has adopted the elements for an intrusion upon seclusion claim as articulated in *Miller v. National Broadcasting Co.* and the Restatement Second of Torts.[310] Accordingly, "[u]nder California law, a claim for intrusion upon seclusion has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person."[311] The first element is satisfied when the individual claiming an invasion of privacy can show that they have "an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source."[312]

Although an individual "cannot have a reasonable expectation of privacy if she consented to the intrusion,"[313] it is well-accepted under California law that "consent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct' and

308. In Re Facebook Biometric Information Privacy Litigation, No.: 3:15-CV-03747-JD, at 6 (N.D. Cal. Feb. 26, 2018) ("As the Illinois legislature found, these procedural protections are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers -- identifiers that cannot be changed if compromised or misused. When an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.").

309. No.: 3:15-CV-03747-JD, at 4 (quoting Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001)).

310. *See* Miller v. Nat'l Broadcasting Co., 187 Cal. App. 3d 1463, 1482 (Cal. App. 1986); RESTATEMENT (SECOND) OF TORTS § 652B (1977).

311. Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (citing Shulman v. Group W Prod., Inc., 18 Cal. 4th 200, 231 (Cal. 1998)).

312. *Id.*

313. *Opperman*, 205 F. Supp. 3d at 1072 (N.D. Cal. 2016) (citing *Hill v. Nat'l Collegiate Athletic Ass'n.*, 7 Cal. 4th 1, 26 (Cal. 1994)).

if the alleged tortfeasor did not exceed the scope of that consent."[314] *Opperman v. Path, Inc.* illustrates consent in intrusion upon seclusion claim.

Opperman involved the adequacy of consumer consent and notice within Yelp's Privacy Policy.[315] Due to an ambiguity in the Privacy Policy, the question in *Opperman* was whether consumer consent to allow Yelp to "find friends" also implies "consent to upload that data to Yelp's servers."[316] The Northern District of California denied Yelp's motion for summary judgment and dismissal, noting that "a reasonable jury could find that Yelp's Privacy Policy provisions do not explicitly address—and thus do not obtain knowing consent" for purposes beyond what was stated in the Privacy Policy.[317] Facebook's Terms of Service and Data Policy are analogous to the consent issues with Yelp's Privacy Policy in *Opperman*, as consumers cannot knowingly consent to something of which they are unaware. Specifically, Facebook users cannot consent to the company collecting their biometric data, since the inclusion of facial recognition technology is not stated in the Terms of Service or Data Policy to which users are required to consent. As such, under an intrusion upon seclusion claim, it would be plausible for California courts to find that Facebook users could not possibly have consented to Facebook's facial recognition data collection from the outset, and that the company exceeded the scope of any proffered consumer consent that it received.

As to the second element of an intrusion upon seclusion claim, "the intrusion must also be 'highly offensive to a reasonable person and sufficiently serious and unwarranted as to constitute an egregious breach of the social norms.'"[318] Significantly, California courts have noted that "[a] 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms."[319] Moreover, California courts have clarified that "community norms" entails that "'[t]he protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.'"[320] For example, in *Opperman*, the Northern District of California said that data collected through invasive or unwanted means needs to be "more private than a person's mailing address" and that the collection needs to be outside of the scope of "routine commercial

314. *Opperman*, 205 F. Supp. 3d at 1072 (quoting RESTATEMENT (SECOND) OF TORTS § 892A, §§ 2(b), 4 (1979)).

315. Opperman v. Path, Inc., 205 F. Supp. 3d 1064 (N.D. Cal. 2016).

316. *Id*. at 1075–76.

317. *Id*. at 1074.

318. *See Opperman*, 205 F. Supp. 3d at 1077 (quoting Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 295 (Cal. 2009)); *see also* Miller v. Nat'l Broadcasting. Co., 187 Cal. App. 3d 1463, 1483–84 (Cal. App. 1986) ("A court determining the existence of 'offensiveness' would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.").

319. *Opperman*, 205 F. Supp. 3d at 1079 (quoting *Hill*, 7 Cal. 4th at 37).

320. *Opperman*, 205 F. Supp. 3d at 1079 (quoting In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014).

behavior."[321] Certainly biometric data is more private than a mailing address, because although you can move and change your address, "you cannot change your fingerprint, and you cannot change your face."[322]

Facebook has far surpassed any kind of "routine commercial behavior" with respect to its facial recognition capabilities, and the company's seemingly endless patent requests using the technology seem to go far beyond any kind of routine commercial activity as well.[323] Of paramount concern is an August 2015 patent filing in which Facebook sought to "utilize passive imaging information" by visually tracking user's emotions and facial expressions across "social networks, news articles, video, audio, or other digital content."[324] The stated purpose of this patent is essentially to bring in advertising revenue, as the patent filing specifies that "advertisement delivery may be customized based upon a user's detected emotions."[325] If offensiveness is truly determined by widely-held community values, then California courts must take into account the fact that despite 93% of Americans reporting the importance of controlling who can access their personal information, only a mere 9% actually feel in control of the extent of information collected about them.[326] Accounting for the 68% of American adults who use Facebook daily,[327] it seems farfetched to believe that allowing highly invasive practices would be considered the social norm. The Northern District of California recently noted that "[t]hose customs and habits are very much in flux,"[328] meaning that California courts can put a stop to Facebook's vastly overstepping of the bounds of consumer consent and privacy before any further irreversible escalation.

It is plain that there are numerous ways for California courts to protect consumers from invasions of privacy without hindering Facebook's foray into more innovative uses for facial recognition technology. California courts have the legal tools available to shift the course and create a pro-privacy and pro-consumer landscape. As continued failure to act will present insurmountable challenges for consumer privacy, Facebook's current facial recognition

---

321. *Opperman*, 205 F. Supp. 3d at 1078 (citation omitted).

322. *Facial Recognition Hearing*, *supra* note 49, at 1 (opening statement of Sen. Al Franken, Chairman of S. Subcomm. on Privacy Tech. and the Law).

323. *See, e.g.*, U.S. Patent No. 20170140214 (filed May 18, 2017) (seeking to capture facial data points in order to generate an emoji based on the user's current facial emotion); U.S. Patent No. 20160127360 (filed May 5, 2016) (seeking to use facial recognition data and speech recognition data for access and authentication into the social media site); U.S. Patent No. 20150242679 (filed Aug. 27, 2015) (discussed *infra*, note 290).

324. *See generally* U.S. Patent No. 20150242679 (filed Aug. 27, 2015) (Facebook is looking to "include emotions or expressions such as a smile, joy, humor, amazement, excitement, surprise, a frown, sadness, disappointment, confusion, jealously, indifference, boredom, anger, depression, or pain").

325. *See* U.S. Patent No. 20150242679 (filed Aug. 27, 2015).

326. *See* George Gao, *What Americans think about NSA, surveillance, national security and privacy*, PEW RESEARCH CENTER (May 29, 2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

327. PEW RESEARCH CENTER, Social Media Fact Sheet (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/social-media/.

328. *Opperman*, 205 F. Supp. 3d at 1079.

practices necessitate significantly overdue judicial intervention from the California judiciary.

V. CONCLUSION

As written, Facebook's Terms of Service and Data Policy wrongfully allows unrestricted collection, disclosure, and use of sensitive biometric identifiers in ways that its users neither understand nor explicitly consent to. California courts would be wise to accept that "[o]paque privacy waivers that consumers merely click through without understanding are no substitute for real and substantive consumer privacy protections in the digital age. Forced consent is not consent at all."[329] Acknowledging that Facebook has everything to gain, and consumer privacy rights have everything to lose, California courts should recognize the very real risk of harm to consumers by Facebook's accumulation and handling of biometric data. Pro-consumer intervention can be achieved under California law through any of the three legal avenues discussed in this note. A pro-consumer privacy holding from California will hopefully spark meaningful policy and legislative changes on both the state and federal levels to adequately address the possible privacy implications from unregulated facial recognition technology. Facebook controls the narrative, but it is not too late for the California judiciary to step in and lead the way by preventing the company from unequivocally controlling consumer privacy, both now and in the future. Without action and interference, there is nothing to stop Facebook from expanding its collection, use and distribution of images in its facial recognition database – all at the expense of over one billion innocent and non-consenting users.[330]

329. *See* MacLean, *supra* note 12, at 46.

330. The author would like to draw attention to a 2010 article featured in The New Yorker, in which it was revealed that Facebook founder Mark Zuckerberg once called the social media site users "dumb fucks" for trusting him with their personal data. *See* Jose Antonio Vargas, *The Face of Facebook*, THE NEW YORKER (Sept. 20, 2010), http://www.newyorker.com/magazine/2010/09/20/the-face-of-facebook [https://perma.cc/LYW9-82FN].

U.S. competitiveness in the 21st century. As a case in point, I focus on broadband technologies (both wired and wireless), which policymakers of all political stripes have identified as crucial for economic growth. In this *Economic Policy Vignette*, I first identify the practical, as opposed to ideological, case for regulatory reform in the broadband sector. I then identify a number of specific measures that present themselves at this moment which create opportunities for meaningful and beneficial regulatory reform.

NOTES

Social Network or Social Nightmare: How California Courts Can Prevent Facebook's Frightening Foray Into Facial Recognition Technology From Haunting Consumer Privacy Rights Forever

Facebook undeniably has extraordinary facial recognition capabilities, so much so that its technology outranks the federal government's facial recognition database in both size and accuracy. Facebook maintains its enormous and eerily precise database by routinely updating and cultivating photos posted nearly every ten seconds by the company's 1.86 billion users. In other words, this feat is accomplished with the help of users like you.

With no comprehensive federal data privacy protection law in place to regulate private industry's use and collection of facial recognition data, Facebook's 1.86 billion users do not suspect the significant privacy implications threatened by the company's vague yet deceptively overbearing Terms of Service and Data Policy. Taken together, these policies bestow upon the social media giant free rein over its users' biometric data and information collected through its use of facial recognition technology.

Facebook simply cannot be trusted to self-regulate, especially when its commercial gain comes at the expense of the privacy of incognizant consumers. "If you don't like it, don't use it" is no longer a sustainable argument. Facebook's brazen and unregulated ability to exploit the biometric identifiers of its billions of users is strictly dependent on both users and courts allowing the company to do so. Yet with only three states espousing applicable biometric collection laws, and a host of other states having nothing to show but failed attempts at regulating facial recognition, legislative efforts simply are not keeping pace with this rapidly evolving technology.

This note seeks to draw attention to the very real problem of Facebook's facial recognition technology capabilities and its subsequent biometric data collection practices outpacing state and federal laws and regulations. This note will assess Facebook's capabilities and practices with respect to facial recognition technology and analyze the related privacy implications for consumers. Through an examination of the company's Terms of Service and Data Policy, this note will demonstrate why California courts should deem Facebook's user agreements unconscionable in order to safeguard consumer privacy rights. In doing so, this note will conclude by offering three plausible legal avenues for the California judiciary to consider to strike down the imperious and heavily invasive terms that Facebook imposes on its users.